



Datenschutzrecht in Hausarztpraxen – Merkblatt für Hausärztinnen / Hausärzte mit Mustertexten und Checklisten

Stand Juli 2026





I. Hintergrund, Bedeutung des Themas für Hausarztpraxen

Mit Inkrafttreten des „neuen“ Datenschutzrechts im Jahr 2018 in Form der [EU-Datenschutz-Grundverordnung](#) (DSGVO) und des novellierten Bundesdatenschutzgesetzes (BDSG) kam es für (Haus-)Arztpraxen zu tiefgreifenden Änderungen: da Patientendaten als „besondere personenbezogene Daten“ (Gesundheitsdaten) besonders schützenswert sind, erfordert die Einhaltung des Datenschutzes strenge technische, organisatorische und administrative Maßnahmen. Bei Nichtbefolgung der Anforderungen drohen auch weiterhin hohe Bußgelder.

Konkret bedeutet dies: (Haus-)Ärztinnen und (Haus-)Ärzte verarbeiten im Rahmen ihrer Tätigkeit Gesundheitsdaten. Hierbei handelt sich um eine „besondere Kategorie personenbezogener Daten“ gem. Art. 9 Abs. 1 DSGVO. Diese Daten sind wegen des Verarbeitungskontextes besonders schutzbedürftig. Gesundheitsdaten sind personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person (Patient/-in) einschließlich der Erbringung von Gesundheitsdienstleistungen beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen. Die DSGVO sieht für die Verarbeitung solcher Daten besondere Regelungen mit erhöhten Rechtmäßigkeitsanforderungen vor: Die Verarbeitung von Gesundheitsdaten muss deshalb nicht nur die allgemeinen Anforderungen von Art. 6 Abs. 1 DSGVO, sondern auch die speziellen Anforderungen von Art. 9 Abs. 2 DSGVO erfüllen.

Im Folgenden sollen die Minimalanforderungen, die an die Einhaltung datenschutzrechtlicher Bestimmungen in Zusammenhang mit der praktischen hausärztlichen Tätigkeit gestellt werden, in Grundzügen erläutert werden. Diese entbinden nicht von einer Prüfung im konkreten Einzelfall und einer jeweiligen Anpassung an die individuellen Gegebenheiten.

II. Allgemeine Hinweise (vgl. Muster „Merkblatt für Patienten“)

Datenschutzrecht betrifft den Schutz von personenbezogenen Daten. Das sind alle Einzelangaben über persönliche oder sachliche Verhältnisse einer Person, insbesondere also Patienten und Mitarbeiter. Beispiele sind Name und Anschrift, Geburtsdatum, Bankverbindung u. ä. Die Art der Erfassung (digital oder auf Papier) spielt keine Rolle. Der Datenschutz bezieht sich auf jede Form des Verarbeitens, also z. B. Erheben, Speichern, Verändern, Übermitteln, Sperren und Löschen.

Nach der DSGVO sind Verarbeitungen grundsätzlich verboten, es sei denn, es besteht eine Erlaubnis im Gesetz. In der Praxis werden Datenverarbeitungen vielfach durch deren Notwendigkeit für die Erfüllung vertraglicher Pflichten (z. B. Behandlungsvertrag, Arbeitsvertrag) gerechtfertigt sein. Schließlich kann eine informierte und freiwillige Einwilligung eingeholt werden.

In jedem Fall muss über die Datenverarbeitung informiert werden, Art. 13 DS-GVO.



Die DSGVO enthält eine Reihe weiterer relevanter Regelungen, wie z. B. die Pflicht zur Erstellung eines Verfahrensverzeichnisses, Pflichten zur IT-Sicherheit, Benachrichtigungspflichten bei Datenpannen, Auskunftsrechte der betroffenen Personen. Bei besonderen datenschutzrechtlichen Gefahrenlagen ist eine sog. Datenschutz-Folgenabschätzung durchzuführen.

CAVE: Weitere allgemeine Informationen mit Mustertexten

- Bayerisches Landesamt für Datenschutzaufsicht, Anforderungen der DSGVO an kleine Unternehmen, Vereine, etc. – Muster 5: Arztpraxis
- KBV, Datenschutz, Datenschutz-Grundverordnung in der Praxis, u. a. Muster: Patienteninfo zum Datenschutz, Muster: Verzeichnis von Verarbeitungstätigkeiten (<https://www.kbv.de/praxis/praxisfuehrung/datenschutz>)



III. Konkrete Schritte

Die folgenden Maßnahmen und Schritte sind das absolute Minimum im Hinblick auf die datenschutzrechtlichen Verpflichtungen der niedergelassenen Hausärztin / des niedergelassenen Hausarztes. Sie ersetzen nicht eine umfassendere Befassung mit dem Thema Datenschutz. Zusätzliche Verarbeitungen, wie z. B. die Durchführung einer Videosprechstunde, erfordern zusätzliche Klärungen und Dokumentation.

1 Verzeichnis von Verarbeitungstätigkeiten (vgl. Muster „Verarbeitungsverzeichnis“)

Art. 30 DSGVO verpflichtet dazu, ein sog. Verzeichnis von Verarbeitungstätigkeiten zu führen. In diesem sind die wesentlichen Verarbeitungstätigkeiten, die verarbeiteten Daten, die Zwecke der Verarbeitung und die Rechtsgrundlage zu dokumentieren. Es schafft so einen Überblick über alle Datenverarbeitungsprozesse der Praxis. Dies erleichtert es z. B., mit Datenschutzvorfällen umzugehen und Anfragen Betroffener zu beantworten.

Hinweis: Dieses kurze Muster soll Verantwortlichen nur den Einstieg in das Thema „Verzeichnis von Verarbeitungstätigkeiten“ gem. Art. 30 Abs. 1 DS-GVO erleichtern. Ein umfassendes Muster ist unter www.lida.bayern.de/media/disk_muster_vov_verantwortlicher.pdf abrufbar.

Bayerisches Landesamt für
Datenschutzaufsicht



Muster 5: Arztpraxis – Verzeichnis von Verarbeitungstätigkeiten

Verantwortlicher:
Dr. Max Hausarzt
Landstr. 3a
87123 Sonsthausen
Tel. 0981/123456-0
E-Mail: team@drhausarzt.de
Web: www.drhausarzt.de

Verarbeitungs- tätigkeit	Ansprechpartner	Datum der Einführung	Zwecke der Verarbeitung	Kategorie betroffene Personen	Kategorie von personenbezogenen Daten	Kategorie von Empfängern	Drittlands- transfer	Löschfristen	Technische/or- ganisatorische Maßnahmen
Lohn- abrechnung	Dr. Max Hausarzt 0981/123456-1 Max@ drhausarztb.de	02.03.2018	- Auszahlung der Löhne/Gehälter - Abfuhr Sozialabgaben u. Steuern	Beschäftigte	- Name, Geburtsdatum - Adresse - Bankverbindungsdaten - Lohn-/Entgeltdaten - ggf. Religionszugehörigkeit - Sozialversicherungsdaten - Steuerdaten (Steuerklasse, Freibeträge) - Berufsgenossenschaftsangaben	Finanzamt	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheitskonzept
Verarbeitung von Patientendaten zur Behandlung	Dr. Max Hausarzt 0981/123456-1 Max@ drhausarztb.de	02.03.2018	Behandlung	Patienten	- Name, Adressen - Gesundheitsdaten - Behandlungsdaten	Vor-, Mit und Nach- behandler	Keine	10 Jahre (gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheitskonzept
Verarbeitung von Patientendaten zur Abrechnung über die KVB bzw. PVS	Sarah Meier 0981/123456-0 sara@drhausarztb.de	28.02.2018	Abrechnung	Patienten	- Behandlungsdaten (Sozial)Versicherungsdaten	- KVB - PVS	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheitskonzept
Betrieb der Webseite mit Möglichkeit der Online- Terminbuchung	Leonhard Kuper 0981/123456-2 Leonhard@Kuper.de	02.03.2018	- Betrieb einer Webseite - Terminbuchung	- Patienten - Webseitenbe- sucher	- IP-Adresse - Name und Kontakt - Grund des Terminwunsches - Terminwunsch	Keine	Keine	IP-Adresse nach 30 Tagen	Siehe IT-Sicherheitskonzept https, sowie bei Terminbuchung Inhaltsverschlüsselung

Auszug aus dem IT-Sicherheitskonzept (enthält technische und organisatorische Maßnahmen):

- ✓ Automatische Updates im Betriebssystem aktivieren
- ✓ Standard-Gruppenverwaltung (z. B. in Windows)
- ✓ PVS und Recherche-PC trennen
- ✓ Automatische Updates des Browsers aktivieren
- ✓ Aktueller Virens Scanner/Sicherheitssoftware
- ✓ Zugriffs- und Berechtigungskonzept
- ✓ Backups regelmäßig, z. B. einmal wöchentlich auf externe Festplatte
- ✓ Papieraktenvernichtung mit Spezial-Shredder
- ✓ Ende-zu-Ende und Transportverschlüsselung bei Onlineterminbuchung (siehe 7. Tätigkeitsbericht BayLDA)

https://www.lida.bayern.de/media/muster_5_arztpraxis_verzeichnis.pdf



CAVE: Weitere allgemeine Informationen und Mustertexte

- Bayerisches Landesamt für Datenschutzaufsicht, Muster 5: Arztpraxis – Verzeichnis von Verarbeitungstätigkeiten
- KBV, Muster: Verzeichnis von Verarbeitungstätigkeiten (<https://www.kbv.de/documents/praxis/praxisfuehrung/datenschutz/datenschutz-verarbeitungsverzeichnis-ausfuellbeispiel.pdf>)
- Datenschutzkonferenz, Kurzpapier 1: Verzeichnis von Verarbeitungstätigkeiten – Art. 30 DS-GVO
- Datenschutzkonferenz, Muster für Erstellung eines Verzeichnisses von Verarbeitungstätigkeiten (Word-Version)

Geeignete technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten (vgl. „Umsetzung technischer und organisatorischer Maßnahmen (TOMs) nach Art. 32 DSGVO unter Berücksichtigung der KBV-IT-Sicherheitsrichtlinie“)

Personenbezogene Daten und ganz besonders Gesundheitsdaten in Arztpraxen sind nicht nur auf rechtlicher Ebene, sondern auch auf technischer und organisatorischer Ebene zu schützen. Die DSGVO schreibt konkrete technisch-organisatorische Maßnahmen im Detail nicht vor. Vielmehr spricht Art.32 DSGVO davon: „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 ... trifft der Verantwortliche geeignete technische und organisatorische Maßnahmen...“ Im organisatorischen Bereich geht es beispielsweise darum, wie der Empfangsbereich der Arztpraxis in datenschutzrechtlicher Hinsicht ausgestaltet sein sollte, z.B. sollte eine Einsichtnahme auf Bildschirme durch wartende Patienten verhindert werden. Technische Maßnahmen zum Datenschutz betreffen oftmals die Software oder auch zum Beispiel die Fragestellung, durch welche Maßnahmen die Patientendaten gegen unbefugten Zugriff geschützt werden können (z. B. Passwortschutz).

CAVE: Weitere allgemeine Informationen, Muster und Checklisten

- Die Landesbeauftragte für den Datenschutz Nordrhein- Westfalen, Technische Anforderungen an technische und organisatorische Maßnahmen beim E-Mail-Versand (<https://www.lidi.nrw.de/technische-anforderungen-technische-und-organisatorische-massnahmen-beim-e-mail-versand>)
- KVN, DSGVO (<https://www.kvno.de/praxis/haeufige-fragen/gesetze/dsgvo>)
- KBV, Aufstellung der Maßnahmen zum Datenschutz (<https://www.kbv.de/praxis/praxisfuehrung/datenschutz>)



2 Datenschutzbeauftragter (vgl. Muster „Benennung eines Mitarbeiters zum DSB“ und „Benennung eines ehrenamtlichen DSB“)

Häufig wird es nicht erforderlich sein, einen Datenschutzbeauftragten zu ernennen, sofern weniger als zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind (merke: „ständig beschäftigt“ ist die Medizinische Fachangestellte; „nicht ständig beschäftigt“ ist die Reinigungsfachkraft, die theoretisch personenbezogene Daten zur Kenntnis nehmen kann). Dies gilt allerdings nur dann, wenn keine überdurchschnittlichen Umfänge oder Intensitäten der Datenverarbeitung erreicht werden.

CAVE: Weitere allgemeine Informationen

- DSK, Kurzpapier Nr. 12: Datenschutzbeauftragte bei Verantwortlichen und Auftragsverarbeitern
- BÄK/KBV, Kapitel 3.9 der Hinweise und Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis, Deutsches Ärzteblatt v. 1. Oktober 2025 (https://www.bundesaerztekammer.de/fileadmin/user_upload/BAEK/Themen/Recht/KBV_BAEK_aerztliche_Schweigepflicht_2025.pdf)

3 Datenschutz-Verpflichtung von Beschäftigten (vgl. Muster „Verpflichtung Einhaltung Anforderungen MFA und VERAH“ und Muster „Verzeichnis von Verarbeitungstätigkeit – Ausfüllhilfe“)

Bei der Aufnahme der Beschäftigung sind Mitarbeitende, die mit personenbezogenen Daten umgehen, zu informieren und dahingehend zu verpflichten, dass die Verarbeitung der personenbezogenen Daten auch durch sie nach den Grundsätzen der DSGVO erfolgt. Hinzu kommt wie bisher die Verpflichtung, Angestellte weiterhin auch nach § 203 StGB zu belehren. Die Belehrungen sollten schriftlich dokumentiert werden.

CAVE: Weitere allgemeine Informationen mit Muster für eine Belehrung

- DSK, Kurzpapier Nr. 19, Unterrichtung und Verpflichtung von Beschäftigten auf Beachtung der datenschutzrechtlichen Anforderungen nach der DS-GVO (https://www.la-bayern.de/media/dsk_kpnr_19_verpflichtungBeschaeftigte.pdf)



4 Auftragsverarbeitung

Sofern Externe in Anspruch genommen werden, um personenbezogene Daten verarbeiten zu lassen, ist ein Vertrag zur Auftragsdatenverarbeitung erforderlich. Die frühere Regelung in § 11 BDSG wurde in Art. 28 DSGVO überführt und erweitert. Ältere Verträge müssen überprüft und ggf. angepasst werden.

Hinzu kommt die Änderung von § 203 StGB im Jahr 2017: Externe müssen infolgedessen nach § 203 StGB belehrt werden, wenn eine Strafbarkeit nach § 203 StGB vermieden werden soll. Die Belehrungen sollten schriftlich dokumentiert werden.

Die großen IT-Dienstleister, u. a. die HÄVG Hausärztliche Vertragsgemeinschaft AG, die seit der Fusion 2025 auch für die HÄVG Rechenzentrum GmbH auftritt, haben – soweit notwendig – die notwendigen Aktualisierungen ihrer Dokumentation vorgenommen.

CAVE: Weitere allgemeine Informationen mit Formulierungshilfen

- Bayerisches Landesamt für Datenschutzaufsicht, Formulierungshilfe für einen Vertrag zur Auftragsverarbeitung
- Datenschutzkonferenz, Kurzpapier Nr. 13 – Auftragsverarbeitung, Artikel 28 DSGVO
- KBV – Datenschutz Grundverordnung
<https://www.kbv.de/praxis/praxisfuehrung/datenschutz>

5 Informations- und Auskunftspflichten (vgl. Muster Merkblatt für Patienten)

Patienteninformation zum Datenschutz in der Praxis

Schon bei der Datenerhebung müssen den betroffenen Personen bestimmte Informationen zur Verfügung gestellt werden. Zum Zwecke der Transparenz müssen Praxen Patientinnen und Patienten daher darüber informieren, was mit deren persönlichen Daten in der Praxis passiert. Mindestens muss darauf hingewiesen werden, wo die Informationen leicht zugänglich sind (z. B. Aushang im Wartezimmer, Auslegen am Empfang, ggf. auch zum Mitnehmen, auf der Homepage, auch als Download). Die Information muss in erster Linie Angaben zum Zweck sowie zur Rechtsgrundlage der Datenverarbeitung enthalten. Auch die Kontaktdaten der Praxis, gegebenenfalls des Datenschutzbeauftragten (sofern eine Pflicht zur Benennung vorliegt bei größeren Praxen, siehe Datenschutzbeauftragter) und des/der Labors/e, mit dem die Praxis zusammenarbeitet, sind anzugeben.

Darüber hinaus haben die betroffenen Personen das Recht, Auskunft über die Verarbeitung ihrer personenbezogenen Daten zu erhalten.



CAVE: Weitere allgemeine Informationen und Muster

- KBV, [Muster für Patienteninformation](#)
- <https://www.kbv.de/praxis/praxisfuehrung/datenschutz>
- Datenschutzkonferenz, [Kurzpapier Nr. 10 – Informationspflichten bei Dritt- und Direkterhebung](#)

Datenschutzhinweise auf Internetseiten oder in Social Media (Facebook, XING, X etc.)

Vielfach nutzen Hausarztpraxen eigene Internet- und/oder sog. Social Media-Seiten zur Präsentation ihrer Praxis und ihrer Angebote / Services.

Solche Seiten **müssen** eine Datenschutzerklärung mit folgenden **Mindestangaben** beinhalten:

Hinweise darauf, dass

- personenbezogene Daten wie Name, Postanschrift, E-Mail-Adresse, Telefonnummer oder das Geburtsdatum ausschließlich in Übereinstimmung mit dem jeweils geltenden Datenschutzrecht erhoben und genutzt werden
- Daten nur gespeichert werden, wenn sie aktiv übermittelt werden
- Daten zum Beispiel nur zur Beantwortung von Anfragen oder zur Zusendung von Informationsmaterial verwendet werden
- Kontaktdaten, die im Rahmen von Anfragen angegeben werden, ausschließlich für die Korrespondenz verwendet werden
- E-Mail-Adressen, die Nutzer für den Bezug eines Newsletters angegeben haben, nur dafür genutzt werden

Es bietet sich zudem an, dass **Merkblatt für Patienten zum Datenschutz** auf der Internetseite der Praxis einzustellen.

Ferner empfiehlt es sich, die inhaltliche Ausgestaltung der Datenschutzerklärung mit dem jeweiligen Provider bzw. IT – Beauftragten abzustimmen.

Allgemeine Muster für Datenschutzerklärungen finden sich zum Beispiel unter <https://www.datenschutz.org/datenschutzerklaerung-website/#datenschutzerklaerung-fuer-eine-website-vorlage-zum-download>



6 Einwilligungserklärungen aktualisieren

Sofern Einwilligungserklärungen verwendet werden, sollten diese durchgesehen und aktualisiert werden. Insbesondere das Thema Freiwilligkeit der Einwilligung und der Hinweis auf das Widerspruchsrecht der Patienten bedürfen einer stärkeren Hervorhebung.

CAVE: Weitere allgemeine und spezifische Informationen

- Bayerisches Landesamt für Datenschutzaufsicht, [Einwilligungen nach der DSGVO](#)
- BÄK/KBV, [Hinweise und Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis](#), Deutsches Ärzteblatt v. 1. Oktober 2025 (unter 2.4.1)

7 Umgang mit Abmahnungen und Geltendmachung von Schadensersatzansprüchen

(Anwaltliche) **Abmahnungen** oder die Geltendmachung von **Schadenersatzansprüchen** – z. B. wegen Verletzung der Informationspflichten nach Art. 13 DSGVO – sind ernst zu nehmen und es empfiehlt sich, selbst **anwaltliche oder sonstige rechtsberatende Hilfe** in Anspruch nehmen!

Was gilt und was ist zu tun:

- Mit einem wegweisenden Urteil vom 27. März 2025 (Az. I ZR 222/19 und I ZR 223/19) hat der BGH endgültig klargestellt, dass Verstöße gegen die DSGVO (z.B. die Informationspflichten aus Art. 13 DS-GVO) **abmahnfähig** sind und von Wettbewerbern (anderen Leistungserbringern) mithilfe ihrer Anwälte nach dem Gesetz gegen den unlauteren Wettbewerb (UWG) verfolgt werden können. **„Wettbewerbliche Abmahnungen“ und Unterlassungsansprüche können auch Hausärztinnen/Hausärzte betreffen.** Praktisch relevant ist auch das Thema „Schadenersatz“:
- **CAVE:** Daneben verlangen viele „Abmahnanwälte“ **Schadenersatz (Art. 82 DSGVO)** bei gleichzeitiger Geltendmachung von **Unterlassungsansprüchen** und **Anwaltsgebühren**. Behauptet wird, dass durch Verletzung von Informationspflichten (Art. 13 DS-GVO), z.B. durch fehlende oder unvollständige Datenschutzerklärungen auf den Homepages, ihren Auftraggebern (Mandanten) ein (immaterieller) Schaden entstanden ist. Tatsächlich liegen in der Regel Rechtsverletzungen und ein Schaden überhaupt nicht vor!
- In diesen Fällen trotzdem und unbedingt **anwaltliche oder rechtsberatende Hilfe in Anspruch nehmen**; dabei auch die meistens sehr kurzen **Fristen beachten** und ggf. die zuständige Rechtsanwaltskammer informieren, wenn Anwälte dieses Vorgehen zu einem „Geschäftsmodell“ entwickelt haben.
- **CAVE: Hinweise unter 6. beachten und umsetzen!**