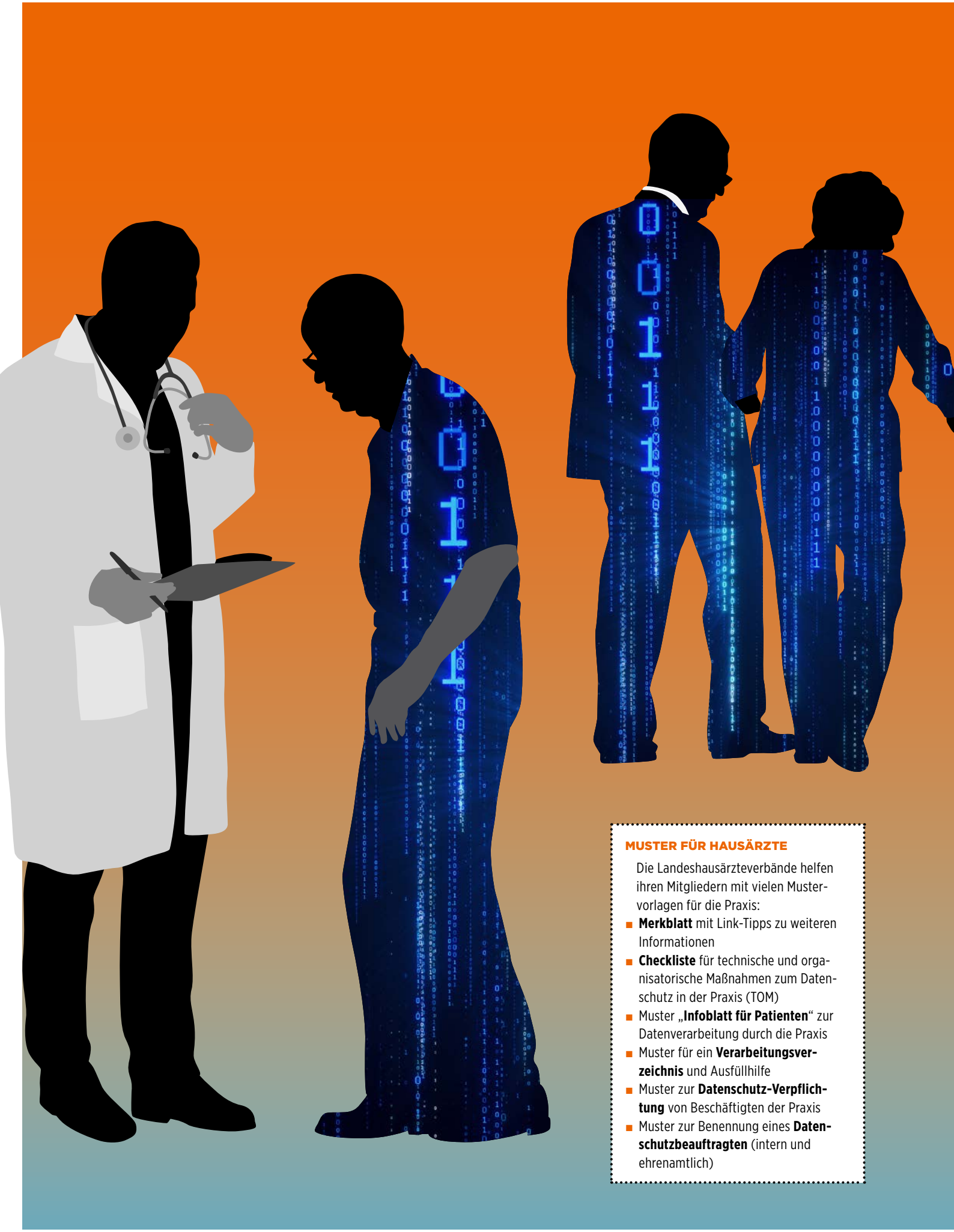

**MUSTER FÜR HAUSÄRZTE**

Die Landeshausärzteverbände helfen ihren Mitgliedern mit vielen Mustervorlagen für die Praxis:

- **Merkblatt** mit Link-Tipps zu weiteren Informationen
- **Checkliste** für technische und organisatorische Maßnahmen zum Datenschutz in der Praxis (TOM)
- Muster „**Infoblatt für Patienten**“ zur Datenverarbeitung durch die Praxis
- Muster für ein **Verarbeitungsverzeichnis** und Ausfüllhilfe
- Muster zur **Datenschutz-Verpflichtung** von Beschäftigten der Praxis
- Muster zur Benennung eines **Datenschutzbeauftragten** (intern und ehrenamtlich)

EU-Recht

# In 7 Schritten zum besseren **Datenschutz**

***Joachim Schütz***
*Geschäftsführer und Justiziar des Deutschen Hausärzteverbands*

Ab 25. Mai gelten für Hausärzte neue Regeln zum Datenschutz. Vor allem die Dokumentations- und Informationspflichten gegenüber Patienten, aber auch Praxismitarbeitern haben sich verschärft. Der Deutsche Hausärzteverband hat dazu ein **Merkblatt und viele Mustervorlagen** erarbeitet.

Noch 20 Tage haben Hausärzte Zeit, um ihre Maßnahmen zum Datenschutz an den Vorschriften der EU-Datenschutzgrundverordnung (DSGVO) auszurichten. Änderungen hat der Deutsche Hausärzteverband in einem Merkblatt zusammengefasst. Dieses stellen die Landeshausärzteverbände samt Mustervorlagen (s. Kasten) für ihre Mitglieder gratis zur Verfügung (meist auch online im Mitgliederbereich). Derzeit konkretisieren sich die Umsetzungshinweise stetig, Hausärzte sollten also weiter ein Auge auf das Thema haben. Der Hausärzteverband wird seine Vorlagen kontinuierlich aktualisieren und über Neuerungen informieren.
Die DSGVO ersetzt das alte Bundesdatenschutzgesetz (BDSG), damit ändern sich für Ärzte die datenschutzrechtlichen Pflichten. Setzen sie die Änderungen nicht um, ist mit höheren Bußgeldern als bisher zu rechnen.

## Um welche Daten geht es?

Verschärft wird der Schutz von **personenbezogenen Daten**: Das sind alle Einzelangaben über persönliche oder sachliche Verhältnisse einer Person wie Name, Anschrift, Geburtsdatum, Gesundheitsdaten, Bankverbindung oder Sozialversicherungsnummer. Im Fokus stehen dabei nicht nur die Patienten, sondern auch das Praxisteam.
Der Datenschutz bezieht sich auf **jede Form des Verarbeitens**, also etwa Erheben, Speichern, Verändern, Übermitteln, Sperren und Löschen. Verarbeitungen sind künftig grundsätzlich verboten, es sei denn, das Gesetz erlaubt dies. Da Ärzte oft Daten verarbeiten müssen, um ihre Vertragspflichten zu erfüllen (Behandlungsvertrag, Arbeitsvertrag), wird die Verarbeitung vielfach bereits gesetzlich gerechtfertigt sein. So ermöglichen etwa Art. 5 und 9 DSGVO i.V.m. Paragraf 22 BDSG-neu die Verarbeitung von Gesundheitsdaten zur ärztlichen Behandlung, zur Erfüllung gesetzlicher Pflichten gegenüber Versicherungsträgern und KV sowie zur Wahrung von Rechtsansprüchen.
Es empfiehlt sich aber, ab sofort Patienten, Mitarbeiter und Dienstleister besser über den Datenschutz und die Verwendung der Daten zu **informieren und freiwillige Einwilligungen** einzuholen. Eine solche Einwilligung sollten Patienten unterzeichnen, wenn sie einen Recall-Service der Praxis nutzen wollen, rät das Landesdatenschutzzentrum Schleswig-Holstein (ULD). Auch für die Zusammenarbeit mit Dienstleistern ist dies oft nötig (s. Schritt 5).

Laut dem Bayerischen Landesamt für Datenschutzaufsicht (BayLDA) sollten Praxischefs ihre Mitarbeiter aufklären, dass sie die DSGVO beachten müssen und sie eine Datenschutz-Verpflichtung unterschreiben sollten (s. Schritt 4). In jedem Fall müssen Praxen aber über die Verarbeitung informieren, legt Art. 13 DSGVO fest. Darüber hinaus sieht die DSGVO weitere Änderungen vor. Welche Maßnahmen sollten Ärzte nun angehen?
**Nächste Schritte in der Praxis:** Die folgenden Maßnahmen sind das Minimum, das Hausärzte umsetzen sollten. Sie ersetzen nicht eine umfassendere Befassung mit dem Thema Datenschutz (s. Links). So haben Bundesärztekammer (BÄK) und Kassenärztliche Bundesvereinigung (KBV) ihre „Hinweise zur Schweigepflicht, Datenschutz und Datenverarbeitung" überarbeitet. Zusätzliche Verarbeitungen, wie eine Videoüberwachung in der Praxis, müssen Ärzte separat klären lassen und dokumentieren.

## 1. Verzeichnis erstellen

Nach Art. 30 DSGVO müssen Praxisinhaber in einem Verzeichnis **alle** (auch manuelle) Verarbeitungstätigkeiten auflisten. Es dokumentiert Vorgänge, wie und welche Daten die Praxis verarbeitet sowie zu welchem Zweck. Dabei sollte man auch an die Praxiswebsite (Kontaktformular, Terminerinnerung per SMS) oder den Facebook-Auftritt denken. Jede Tätigkeit braucht ein eigenes Verzeichnis – also ein Verzeichnis für das Arbeiten im PVS, eines für das Erstellen der Personalakten. Der Hausärzteverband hat dazu ein Muster samt Ausfüllhilfe erarbeitet.
**Faustregel:** Praxen sollten Daten nur so lange aufbewahren, wie dies für die Behandlung und laut Gesetz nötig ist. Meist sollte man sie zehn Jahre nach Ende der Behandlung löschen, wobei Fachgesetze oder die Verjährung möglicher Haftungsansprüche (BGB) längere Zeiträume vorgeben können (etwa für Röntgenaufnahmen). Sobald die Rechtsgrundlage entfällt, sollte man die Daten vernichten (Fristen s. Link).
Achten Sie beim Anlegen des Verzeichnisses darauf, ob Sie Verarbeitungen „mit besonders hohem Risiko" vornehmen (etwa Videoüberwachung der Praxis). In diesem Fall brauchen Sie eine Datenschutz-Folgenabschätzung und einen Datenschutzbeauftragten.
BÄK und KBV raten Ärzten zudem, eine Datenschutzrichtlinie zu erstellen. Sie dokumentiert Verantwortlichkeiten, Zugriffsrechte der Mitarbeiter, die Erfassung von Daten oder die Rechtsgrundlage. So kann man dort etwa den Ablauf und den Verantwortlichen festlegen, der sich um die Meldung einer Datenpanne kümmert (Schritt 2).

### LINK

Weitere Infos im Netz:

- Hinweise zum Datenschutz und technische Anlage von BÄK und KBV: **https://hausarzt.link/inGSl**
- Kurzpapiere der Datenschutzkonferenz: **https://hausarzt.link/F2w1y**
- „Datenschutz-Check 2018" von BÄK und KBV: **https://hausarzt.link/m0h0L**
- Aufbewahrungsfristen: **https://hausarzt.link/UGypg**
- Der Berufsverband der Datenschutzbeauftragten Deutschlands sammelt weitere Muster, z.B. zur Datenschutzerklärung für Websitebetreiber, zum Datenschutz bei Beschäftigten oder zur Auftragsdatenverarbeitung: **www.bvdnet.de/bvd-arbeitskreise/arbeitskreis-medizin**

## 2. IT-Sicherheit prüfen

Die DSGVO erhöht die Anforderungen an die IT-Sicherheit. BÄK und KBV überarbeiten derzeit die technische Anlage zu den Datenschutz-Hinweisen. Wie bisher sollten Praxen **technisch-organisatorische Maßnahmen** ergreifen, um einem Missbrauch vorzubeugen. So sollte man einen „Internetrechner" installieren, der nicht mit den Patientendaten vernetzt ist. Der Hausärzteverband hat dazu die Checkliste TOM verfasst (S. 20).
Hinzu kommen Informationspflichten bei **Datenpannen**: Hackerangriffe, Fehlversand von Arztbriefen oder versehentliches Löschen von Daten müssen Ärzte in bis zu 72 Stunden an die Aufsichtsbehörde (Übersicht: https://hausarzt.link/64Fqc) melden. Das BayLDA rät, Praxen sollten den Ablauf üben, damit klar ist, wer Aufsichtsbehörde und Betroffenen informiert sowie Maßnahmen einleitet.
Ärzte sollten ihre Hard- und Software regelmäßig aktualisieren, um Fehler zu beseitigen.

## 3. Datenschutzbeauftragter

Oft werden Praxen keinen Datenschutzbeauftragten brauchen, sofern weniger als zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. Dies gilt, wenn man keine überdurchschnittlichen Umfänge oder Intensitäten der Datenverarbeitung erreicht. **Merke:** „Ständig beschäftigt" ist die MFA, „nicht ständig beschäftigt" ist die Reinigungskraft, die theoretisch Personendaten zur Kenntnis nehmen kann.

Fotos: A-Digit - iStockphoto

## 4. Datenschutz-Verpflichtung von Beschäftigten einholen

Bei der Aufnahme der Beschäftigung müssen Praxisinhaber ihre Beschäftigten, die mit personenbezogenen Daten umgehen, informieren und verpflichten, dass sie die DSGVO einhalten (mehr: https://hausarzt.link/7nUGw). Hinzu kommt wie bisher die Verpflichtung, Angestellte nach Paragraf 203 StGB (Verstoß gegen das Patientengeheimnis) zu belehren. Die Belehrungen sollten Praxisinhaber dokumentieren (Muster S. 20).

## 5. Auftragsverarbeitung prüfen

Viele Praxen haben die Wartung ihrer EDV oder das Vernichten von Akten ausgelagert. Sind personenbezogene Daten betroffen, braucht es einen Vertrag zur Auftragsdatenverarbeitung (Art. 28 DSGVO). Hausärzte müssen ihre **Verträge prüfen und anpassen**. Unnötig ist ein solcher Vertrag laut KBV bei Terminservicestellen, der rein technischen IT-Wartung (Kühlung, Stromzufuhr) oder zur Zusammenarbeit mit Steuerberatern, Rechtsanwälten oder Wirtschaftsprüfern. Neu ist, dass Ärzte externe Dienstleister nach **Paragraf 203 StGB** belehren müssen, um eine Strafbarkeit nach Paragraf 203 StGB zu vermeiden. Die Belehrungen sollten Ärzte schriftlich dokumentieren.
Große IT-Dienstleister, HÄVG Rechenzentrum GmbH und HÄVG Hausärztliche Vertragsgemeinschaft AG haben ihre Dokumentation aktualisiert und stellen diese, soweit notwendig, rechtzeitig zur Verfügung. Von dort erhalten an der Hausarztzentrierten Versorgung (HZV) teilnehmende Hausärzte mehr Informationen.

## 6. Betroffene informieren

Schon bei der Datenerhebung muss man den Betroffenen bestimmte Informationen zur Verfügung stellen. Denn nur, wer seine Rechte kennt, kann diese wahrnehmen. Die HÄVG gibt HZV-Teilnehmern hierzu Info-Texte an die Hand. Bei der Aufnahme könne das Praxisteam jedem die **Patienteninfo mitgeben und dies im PVS notieren**, sagt das ULD. Am Telefon müsste man diese zwar nicht vorlesen, ein Praxis-Aushang allein reiche aber nicht. Mindestens müssen Ärzte darauf hinweisen, wo die Informationen leicht zugänglich sind (z. B. Flyer, Webseite). Genaue Vorschriften, wie Ärzte informieren müssen, lagen von den Aufsichtsbehörden bis Redaktionsschluss nicht vor. Laut ULD sollte man über Kontaktdaten von Verantwortlichen (z.B. Praxisinhaber) und Datenschutzbeauftragtem, Umfang, Zweck, Dauer und Rechtsgrundlage der Verarbeitung aufklären.
Zudem sollte man über das **Recht auf Auskunft**, Berichtigung, Löschung, Beschwerde und Widerspruch informieren. Das BayLDA rät, einen Ablauf zu erarbeiten und zu üben, wie man Patienten innerhalb eines Monats Auskunft geben kann. Tests zeigten, dass viele Praxen dies nicht schafften, weil die Daten teils aus verschiedenen Speichermedien zusammengetragen werden müssten. Der Patient habe Anspruch auf eine kostenfreie Kopie seiner personenbezogenen Daten.

## 7. Aktualisieren der Einwilligungserklärungen

Ärzte dürfen nur zu bestimmten Zwecken die Patientendaten Dritten offenbaren (Schritt 1 und Hinweise von BÄK und KBV). In anderen Fällen müssen sie zunächst die Einwilligung der Betroffenen einholen, etwa zur Weitergabe an ärztliche Verrechnungsstellen. Verwendet eine Praxis Einwilligungserklärungen, sollten sie diese durchsehen und aktualisieren. Insbesondere die „Freiwilligkeit der Einwilligung“ sollten sie künftig stärker hervorheben. *(Mitarbeit jvb)*

### FAZIT

- Hausärzte sollten spätestens jetzt beginnen, ihre Maßnahmen zum Datenschutz zu prüfen und anzupassen, damit sie den schärferen Regeln der DSGVO gerecht werden.
- Ihr Hausärzteverband unterstützt Sie als Mitglied mit einem Merkblatt, einer Checkliste zu technisch-organisatorischen Maßnahmen und vielen Mustervorlagen (S. 20).
- Die Aufsichtsbehörden arbeiten stetig daran, wie die DSGVO auszulegen ist. Hausärzte sollten daher auch nach dem 25. Mai den Datenschutz im Blick behalten. Der Hausärzteverband wird über weitere Neuerungen informieren.