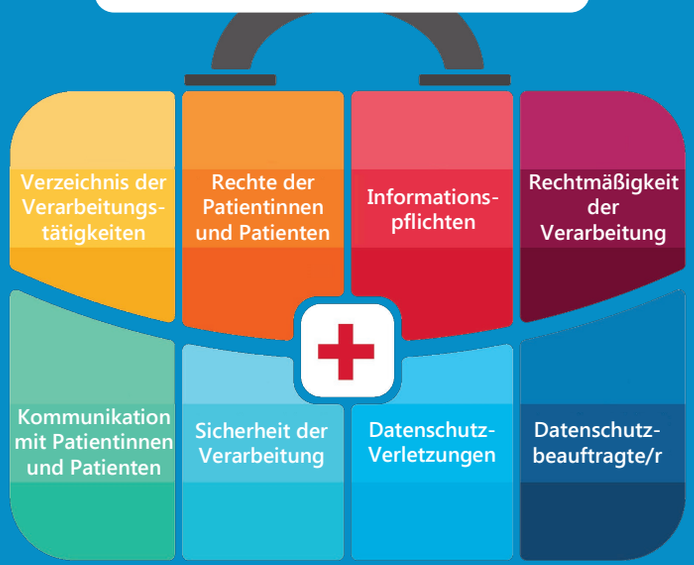
Top 10 der wichtigsten Punkte

- *Verarbeitungsvorgänge überprüfen*
- *Verzeichnis der Verarbeitungstätigkeiten erstellen*
- *Datenschutzbeauftragte/r erforderlich?*
- *Beschäftigte sensibilisieren*
- *Informationspflichten erfüllen*
- *Betroffenenrechte beachten (Auskunft, Löschung)*
- *Verträge zur Auftragsverarbeitung erforderlich?*
- *Webseite überprüfen und sicher halten*
- *Sicherheit der Datenverarbeitung umsetzen*
- *Datenpannen einfach online melden*

Erläuterungen hierzu finden Sie auf
www.lda.bayern.de/top10

Zentrale Datenschutzthemen



Unser Webangebot für Sie:

Mehr Informationen unter
www.lda.bayern.de

HERAUSGEBER
Bayerisches Landesamt für Datenschutzaufsicht
Promenade 27 (Schloss)
91522 Ansbach

Bayerisches Landesamt für Datenschutzaufsicht

Datenschutz für Bayern

DS-GVO einfach umgesetzt in Arztpraxen

Zielgruppe dieses Flyers

Der Fokus dieses Flyers liegt auf **kleineren Arztpraxen**.

Viele der genannten Datenschutzanforderungen können auch auf andere Einrichtungen, die ebenfalls Daten von Patientinnen und Patienten verarbeiten, übertragen werden, wie z. B. Physiotherapiepraxen.

INFORMATIONSPFLICHTEN

In der Arztpraxis müssen Patientinnen und Patienten bei der Datenerhebung bestimmte Informationen über die Verarbeitung ihrer Daten gegeben werden.

Es empfiehlt sich, z. B. durch einen kompakten **Aushang** in der Praxis, dieser Informationspflicht nachzukommen und einen kleinen **Flyer** bzw. ein **Informationsblatt** anzubieten. Sollten auch auf der eigenen **Praxis-Homepage** personenbezogene Daten verarbeitet werden, ist dies dort im Rahmen einer Datenschutzerklärung kenntlich zu machen.

SICHERHEIT DER VERARBEITUNG

Um sensible Patientendaten zu schützen, müssen Arztpraxen über die Standardsicherheitsmaßnahmen hinaus auch geeignete Verschlüsselungstechniken nutzen. Der Einsatz **aktueller Betriebssysteme**, **Passwortschutz** an den Arbeitsplätzen und **Backups** sind dabei das A und O.

Damit Unbefugte nicht an die schutzwürdigen Daten herankommen, sind die Patientendatenbanken selbst besonders abzusichern. Praxisverwaltungssysteme unterstützen meist eine **verschlüsselte Speicherung** der Patientendaten.

VERZEICHNIS DER VERARBEITUNGSTÄTIGKEITEN

Arztpraxen gehen im Alltag mit vielen personenbezogenen Daten um, insbesondere mit den Daten ihrer Patientinnen und Patienten. Deshalb besteht auch für Ärztinnen und Ärzte die **gesetzliche Verpflichtung**, ein Verzeichnis der Verarbeitungstätigkeiten zu führen.

Aus diesem ist dann ersichtlich, welche Daten (Kategorien) zu welchem Zweck verarbeitet werden.

Wie so etwas aussehen kann, zeigt das BayLDA in einem **Muster-Verzeichnis** für kleinere Arztpraxen auf der Webseite.

RECHTMÄßIGKEIT DER VERARBEITUNG

Für die Verarbeitung von Daten im Rahmen der Behandlung von Patientinnen und Patienten ist eine Einwilligung in aller Regel nicht erforderlich. Rechtsgrundlage hierfür ist vielmehr der Behandlungsvertrag.

Eine Einwilligung ist nur in Ausnahmefällen einzuholen, beispielsweise wenn die Abrechnung von Behandlungskosten über eine **private Verrechnungsstelle** erfolgt.

DATENSCHUTZVERLETZUNGEN

Kommt es in der Arztpraxis zu Sicherheitsvorfällen im Umgang mit personenbezogenen Daten, so besteht eine **gesetzliche Meldepflicht** beim BayLDA als Aufsichtsbehörde.

Beispiele solcher Datenschutzverletzungen:

- Diebstahl oder Verlust eines Notebooks
- Fehlversendung eines Arztbriefes
- Verschlüsselungstrojaner per E-Mail

Die Patientinnen und Patienten sind übrigens nur zu informieren, wenn ein hohes Datenschutzrisiko besteht (was die Ausnahme ist).

RECHTE DER PATIENTINNEN UND PATIENTEN

Patientinnen und Patienten haben verschiedene sog. **Betroffenenrechte** nach der DS-GVO, u. a. das Recht auf **Auskunft** und das Recht auf **Löschung**. Auch unabhängig von einem Antrag der Betroffenen sind Daten nach Ablauf gesetzlicher Aufbewahrungsfristen i. d. R. zu löschen.

Um diesen Pflichten nachzukommen, sollten in Arztpraxen bereits entsprechende Verfahren geschaffen werden.

KOMMUNIKATION MIT PATIENTINNEN UND PATIENTEN

Insbesondere wenn sensible Daten übermittelt werden, wie beispielsweise in Befunden enthalten, sind Maßnahmen zum Schutz vor unbefugter Kenntnisnahme zu ergreifen.

Ein Austausch per **E-Mail** oder per **Kontaktformular** über die eigene Homepage ist möglich, wenn neben der Transportverschlüsselung (TLS) auch Möglichkeiten für eine Inhaltsverschlüsselung angeboten werden.

DATENSCHUTZBEAUFTRAGTE/R (DSB)

Ein/e DSB ist insbesondere zu benennen, wenn in der Regel **mindestens zehn Personen ständig** mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind.

Die übrigen Fälle, die die Benennung einer/s DSB erfordern, sind bei kleineren Arztpraxen nur sehr selten gegeben.