



Der Landesbeauftragte für  
**DATENSCHUTZ** und  
**INFORMATIONSFREIHEIT**  
Mecklenburg-Vorpommern

# Fit für den Datenschutz

Hilfen für Ihren Praxisalltag

---

**Heike Thielmann**

**Referentin Gesundheit und Soziales**

c/o Der Landesbeauftragte für Datenschutz und  
Informationsfreiheit Mecklenburg-Vorpommern

# Unsere Agenda für heute

---



## Grundlagen

1x1 des Datenschutzes

## Terminvereinbarungstools

Welches Tool zur Terminvereinbarung über das Internet setzen Sie ein oder wollen Sie zukünftig benutzen? Wir besprechen die datenschutzrechtlichen Anforderungen - was geht und was geht nicht.

# Wann gilt die DSGVO\* eigentlich?

## Für Informationen,

- die ganz oder teilweise automatisiert verarbeitet werden,
- die sich auf eine identifizierte oder **identifizierbare** natürliche Person beziehen, z.B. Namen, KV-Nummer, LANR-Arztnummer, medizinische Befunde einschließlich Abbildungen, aber auch IP-Adressen

## Die DSGVO gilt **nicht**,

- bei ausschließlich persönlichen oder familiären Tätigkeiten
- bei der Ermittlung, Aufdeckung und Verfolgung von Straftaten

\* Datenschutzgrundverordnung

# Das Grundprinzip im Datenschutz

	Datenverkehr	Straßenverkehr
Ziel	Artikel 1 (2) DS-GVO Diese Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten.	§ 1 (2) StVO Wer am Verkehr teilnimmt, hat sich so zu verhalten, dass kein anderer geschädigt, gefährdet oder, mehr als nach den Umständen unvermeidbar, behindert oder belästigt wird.
Grundsatz	Was nicht erlaubt ist, ist verboten.	Was nicht verboten ist, ist erlaubt.

## **Personenbezogene Daten dürfen verarbeitet werden, wenn**

- die betroffene Person ausdrücklich eingewilligt hat,
- die Verarbeitung für die Erfüllung eines Vertrages erforderlich ist (Behandlungsvertrag),
- die Verarbeitung für die Erfüllung einer rechtlichen Verpflichtung erforderlich ist (SGB),
- die Verarbeitung erforderlich ist, um lebenswichtige Interessen der betroffenen Person (oder einer anderen) zu schützen (Schutz des Lebens und der körperlichen Unversehrtheit),
- die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt (öffentliche Gesundheit),
- die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen erforderlich ist (Durchsetzung von Rechtsansprüchen; gilt nicht für Behörden) .

- Strafgesetzbuch (§ 203 StGB Berufs- bzw. Amtsgeheimnis)
- BGB (§ 1358 BGB Notvertretungsrecht für Ehegatten)
- Berufsordnung der Zahnärztekammer Mecklenburg-Vorpommern
- Bundesmantelvertrag – Zahnärzte (BMV-Z)
- alle Sozialgesetzbücher
- Infektionsschutzgesetz (§§ 6 ff. IfSG)
- Gesetz zur Kooperation und Information im Kinderschutz (KKG)
- Gesetz über die Krebsregistrierung in MV (KrebsRG M-V)
- Strahlenschutzrecht (StrlSchG, StrlSchV)

**Die Verarbeitung besonderer Kategorien personenbezogener Daten** (Art. 9 DSGVO) ist grundsätzlich verboten.

## **Besondere Kategorien**

Genetische Daten

Gesundheitsdaten

Daten zum Sexualleben und zur sexuellen Orientierung

Für die Verarbeitung müssen zusätzlich die Anforderungen erfüllt sein:

- Schutz lebenswichtiger Interessen (Notfallversorgung)
- **Versorgung oder Behandlung im Gesundheits- oder Sozialbereich (Behandlungsvertrag)**
- öffentliches Interesse im Bereich der öffentlichen Gesundheit (Corona-Abwehrmaßnahmen)

Verantwortliche, deren **Kerntätigkeit die Verarbeitung besonderer Kategorien personenbezogener Daten** (Art. 9 DSGVO) ist müssen einen **Datenschutzbeauftragten** bestellen\*.

Nach Art. 37 Abs. 1 lit. a – c DS-GVO ist auf jeden Fall ein DSB zu benennen, wenn eine der folgenden Voraussetzungen gegeben ist:

...

c) Kerntätigkeit mit umfangreicher Verarbeitung besonders sensibler Daten (Artikel 9, 10 DS-GVO).

\*Rechtlicher Erläuterung : Es ist unstrittig, dass die Verarbeitung von besonders sensiblen Daten die Kerntätigkeit in Arzt- und Zahnarztpraxen ist. Die Regelung in Art. 37 Abs. 1 DS – GVO geht der nationalen Regelung im Bundesdatenschutzgesetz (§ 38 BDSG) vor. Hier heißt es folgerichtig: "Ergänzend zu Art. 37 Absatz 1 Buchstabe b und c der DSGVO benennen Verantwortliche ...einen Datenschutzbeauftragten, soweit in der Regel 20 Personen ..."



# Wofür sind Sie verantwortlich?

## TRANSPARENZPFLICHT

Nach **Art. 13, 14 DSGVO** müssen betroffene Personen **vor** der Datenerhebung informiert werden.

### Aushändigung Information an den Patienten mit folgenden Inhalten

- Information zum Verantwortlichen (Name, Anschrift)
- Datenschutzbeauftragter (ab 10 Mitarbeitende einschließlich Ärzte)
- Zweck der Verarbeitung
- Rechtsgrundlage für die Verarbeitung
- Empfänger der personenbezogenen Daten (eingeschränkt durch § 82 SGB X)
- Speicherdauer
- Information über Betroffenenrechte

[Muster Patienteninformation Datenschutz von der KBV](#)

# Wofür sind Sie verantwortlich?

## AUSKUNFTSPFLICHT

Nach **Art. 12, 15 DSGVO** müssen betroffene Personen Auskunft über die von Ihnen verarbeiteten Daten erhalten.

Der EuGH (Urteil vom 4. 5. 2023 - C-487/21 und EuGH (1. Kammer) Urteil vom 26.10.2023 – C-307/22 (FT/DW) hat in ständiger Rechtsprechung klargestellt, dass Art. 15 Abs. 3 DS-GVO dahingehend auszulegen ist, „dass das Recht, vom für die Verarbeitung Verantwortlichen eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zu erhalten, bedeutet, dass der betroffenen Person eine originalgetreue und verständliche Reproduktion aller dieser Daten ausgefolgt wird. Dieses Recht setzt das Recht voraus, eine Kopie von Auszügen aus Dokumenten oder gar von ganzen Dokumenten oder auch von Auszügen aus Datenbanken, die u. a. diese Daten enthalten, zu erlangen, wenn die Zurverfügungstellung einer solchen Kopie unerlässlich ist, um der betroffenen Person die wirksame Ausübung der ihr durch diese Verordnung verliehenen Rechte zu ermöglichen, wobei insoweit die Rechte und Freiheiten anderer zu berücksichtigen sind.“

### Anforderungen

- Innerhalb eines Monats nach Eingang des Auskunftsbegehrens
- Vollständig
- So wie es der Patient wünscht – Papier, elektronisch, ggf. Einsichtnahme
- Erste Auskunft kostenfrei

## NACHWEISPLICHT

Führen eines Verzeichnisses aller Verarbeitungstätigkeiten gem. **Art. 30 DSGVO**

Gründe:

- Grundlage für die Erstellung von Datenschutzerklärungen und die Umsetzung von Betroffenenrechten, wie z.B. dem Auskunftsrecht
- Risiken bei der Verarbeitung personenbezogener Daten besser erkennen und geeignete Maßnahmen ergreifen
- Überblick über die verschiedenen Datenverarbeitungsvorgänge zu behalten und Verantwortlichkeiten zu klären, z.B. mit Auftragsverarbeitern

Prozesse

- Verarbeitungsprozess Behandlung
- Verarbeitungsprozess Verwaltung Mitarbeitende
- ggf. Praxismanagementsoftware, wie Online-Terminvereinbarung, Patientenaufruf, Upload für Bilder
- technische Geräte, Datenübertragung in Drittländer

Muster Verzeichnis für Verarbeitungstätigkeiten und Ausfüllhilfe der KBV

[https://www.kbv.de/media/sp/Praxisinformation\\_Datenschutz\\_Verarbeitungsverzeichnis\\_Muster.docx](https://www.kbv.de/media/sp/Praxisinformation_Datenschutz_Verarbeitungsverzeichnis_Muster.docx)

## TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN (TOM)

Sie sind für die Sicherheit der Verarbeitung gem. **Art. 32 DSGVO** verantwortlich .

### Maßnahmen

Verpflichtung der Mitarbeitenden zur Verschwiegenheit (§ 203 StGB)

Verpflichtung der Mitarbeitenden auf die Datenschutzgrundsätze

**Schriftliche** Weisungen zur Datenverarbeitung für Mitarbeitende

- Wie gehe ich mit den Gesundheitsdaten (Praktische Anweisungen)?
- Wie informiere ich über die Datenverarbeitung?
- Was ist bei der Geltendmachung von Betroffenenrechten (Auskunft /Löschung) zu tun?
- Wie verhalte ich mich bei einer Datenpanne (falsch versendete Dokumente)?

Verträge zur Auftragsverarbeitung, z.B. mit dem IT-Dienstleister

[Formulierungshilfe für AV-Vertrag](#)

# Wofür sind Sie verantwortlich?

## Beispiele für schriftliche Weisungen an die Mitarbeitenden

- Patientendaten werden niemals unverschlüsselt über das Internet versendet, beispielsweise per E-Mail.
- Zugriffsberechtigungen sind vergeben; somit ist klar geregelt, wer in der Praxis auf welche Dateien und Ordner zugreifen kann.
- In den Praxisräumlichkeiten wird auf Diskretion geachtet: Die Anmeldung sollte getrennt zum Wartebereich angeordnet sein. Möglich ist auch, Patientinnen und Patienten beispielsweise mit einem Schild darauf hinzuweisen, dass sie am Tresen Abstand halten sollen, wenn mehrere Personen dort warten.
- Patientenakten werden sicher verwahrt.
- Die Computer sind passwortgeschützt, die automatische Bildschirmsperre ist aktiviert.
- Patientenunterlagen werden stets so positioniert, dass andere Patientinnen und Patienten diese nicht einsehen können.
- Wenn der Arzt nicht im Raum ist, werden Patientenakten generell unter Verschluss gehalten.
- Vertrauliche Arzt-Patienten-Gespräche finden stets in geschlossenen Räumen statt.
- Bei Auskünften am Telefon wird die Identität der Anruferin oder des Anrufers gesichert, zum Beispiel durch gezielte Zusatzfragen oder einen Rückruf.

# Wofür sind Sie verantwortlich?

## VERPFLICHTUNG ZUR DATENLÖSCHUNG

Grundsatz der Speicherbegrenzung nach **Art. 5 DSGVO**

Personenbezogene Daten dürfen nicht länger gespeichert werden, als sie benötigt werden.

- Gesetzliche Aufbewahrungsfristen machen die Speicherung von Patientenakten notwendig, z.B. § 10 (2) BOÄ M-V „zehn Jahren nach Abschluss der Behandlung“.
- Ein Arbeitgeber muss Personalakten so lange aufbewahren, wie ein ausgeschiedener Mitarbeitender arbeitsrechtliche Ansprüche geltend machen könnte. Maßgeblich ist hier die in § 195 BGB festgelegte regelmäßige Verjährungsfrist von drei Jahren.
- Es ist festgelegt, wann und durch wen personenbezogene Daten gelöscht beziehungsweise vernichtet werden, sobald die Aufbewahrungsfrist abläuft.

## 1. Zulässigkeit der Auslagerung der Terminverwaltung

- kann als Auftragsverarbeitung im Sinne von Art. 28 DS-GVO zulässig sein
- bedarf auf dieser Grundlage keiner Einwilligung durch die Patientinnen und Patienten
- allerdings sind die die Patientinnen und Patienten über die Einbindung des Dienstleisters zu informieren (Art. 13 DS-GVO, S.U.).

## 2. Anforderungen an eine datenschutzkonforme Verarbeitung von Patientendaten im Zusammenhang mit der Terminvergabe

- **Nur erforderliche Datenverarbeitungen sind ohne Einwilligung zulässig. Erforderlich im datenschutzrechtlichen Sinne bedeutet, dass die Daten für das Terminmanagement unbedingt notwendig sein müssen.**
- das Eintragen von Patientendaten in einem Terminkalender ist für die Behandlung erforderlich, wenn die konkrete Patientin oder der konkrete Patient einen in der Zukunft liegenden Termin in der Praxis vereinbart.
- Eingetragen werden dürfen nur diejenigen Patientendaten, die zur Wahrnehmung des konkreten Termins erforderlich sind, also insbesondere Name, Geburtsdatum, behandelnde Ärztin oder behandelnder Arzt, Behandlungsanlass (z. B. Kontrolle, Röntgen) und eine Kontaktmöglichkeit zur eventuell notwendigen kurzfristigen Absage des Termins.

- **Keine pauschale Übermittlung aller Patientenstammdaten an den Dienstleister im Vorfeld**

Zur Durchführung der Terminvergabe durch einen Dienstleister bedarf es nur der zur Vereinbarung eines konkreten Termins erforderlichen Patientendaten. Diese Daten werden bei einer Online-Terminvereinbarung regelmäßig durch die Patientinnen und Patienten selbst mitgeteilt oder bei einer Terminvereinbarung vor Ort oder telefonisch durch die Arztpraxis erhoben und in den Terminkalender eingetragen. Vor diesem Hintergrund bedarf es im Vorfeld im Regelfall insoweit keiner pauschalen Bereitstellung von Stammdaten aller in der Arztpraxis jemals behandelten Patientinnen und Patienten an das beauftragte Dienstleistungsunternehmen.

- **Terminnachrichten nur mit ausdrücklicher Einwilligung**

Für die Wahrnehmung des konkreten Termins **nicht erforderlich**, allerdings als erweitertes Serviceangebot durchaus denkbar, ist die Versendung einer an die Patientinnen und Patienten gerichteten Terminnachricht (z. B. Terminerinnerung). Sofern die Patientinnen und Patienten auf Nachfrage und entsprechend informiert damit einverstanden sind, dürfen die zu diesem Zweck erforderlichen Kontaktdaten – je nach gewähltem Kommunikationskanal – zusätzlich verarbeitet werden. Die Arztpraxis muss nachweisen können, dass die Einwilligung vorliegt.

- **Keine Datenverarbeitung von Patientendaten, die Gegenstand der Auftragsverarbeitung sind, zu eigenen Zwecken des Terminverwaltungsunternehmens**

Eine weitere Verarbeitung der im Terminkalender eingetragenen Patientendaten durch das Terminverwaltungsunternehmen zu eigenen Zwecken ist regelmäßig unzulässig. Bei Kenntnis einer Verwendung der Patientendaten für eigene Zwecke des Dienstleisters ist die Arztpraxis verpflichtet, gegenüber ihrem Dienstleister dafür zu sorgen, dass dieser einen datenschutzkonformen Zustand herstellt.



- **Eintragungen im Terminkalender sind innerhalb einer kurzen Frist nach dem Termin zu löschen**

Die zur Terminvergabe zulässigerweise erhobenen Patientendaten dürfen nur solange gespeichert werden, wie dies zur Erreichung des Verarbeitungszwecks erforderlich ist. Sobald der in den Terminkalender eingetragene Termin verstrichen ist, besteht im Regelfall keine Erforderlichkeit mehr, in dem Terminkalender weiterhin die Termindaten des Patienten oder der Patientin zu speichern. Denn Eintragungen im Terminkalender sind nicht Teil der Behandlungsdokumentation und unterliegen somit nicht der berufsrechtlichen Dokumentationspflicht. Diese Daten sind deshalb grundsätzlich innerhalb einer kurzen Frist aus dem Terminkalender zu löschen. Erfolgt die Terminvergabe durch einen beauftragten Dienstleister, hat dieser die erforderliche Löschung zu gewährleisten.

- **Besondere Anforderungen bei einer Datenverarbeitung in Drittstaaten (außerhalb der EU)**

Sofern in die Datenverarbeitung zur Terminvergabe und -verwaltung auch Stellen in einem Drittland i.S.v. Art. 44 DS-GVO eingebunden sind, müssen die in diesem Zusammenhang bestehenden besonderen datenschutzrechtlichen Anforderungen der Art. 44 ff. DS-GVO durch die Arztpraxen als Verantwortliche sichergestellt werden.

Vor der Auftragsvergabe ist daher durch die Praxen mit dem Dienstleister zu klären, ob einzelne Verarbeitungsschritte, wie z. B. Support, Wartung oder Administration, in einem Drittland stattfinden und ob in diesem Fall die o. g. Anforderungen erfüllt sind.

### 3. Vertragsverhältnis zwischen Patientinnen und Patienten mit Dienstleistern zur Online-Terminbuchung

Sofern einzelne Terminverwaltungsunternehmen ihre Dienstleistung in der Art anbieten, dass die Patientinnen und Patienten zunächst die AGB des Dienstleisters akzeptieren oder ein Nutzerkonto bei dem Unternehmen anlegen müssen, ist die damit zusammenhängende Verarbeitung personenbezogener Daten durch das Terminverwaltungsunternehmen von der unter Nr. 2 dargestellten Datenverarbeitung im Auftrag der Arztpraxen abzugrenzen.

Für die Verarbeitung personenbezogener Daten von Patientinnen und Patienten im Zusammenhang mit dem Vertrag, den sie mit dem Terminverwaltungsunternehmen schließen, und dem Nutzerkonto ist das Terminverwaltungsunternehmen datenschutzrechtlich Verantwortlicher.

Dem Terminverwaltungsunternehmen obliegt insoweit die Erfüllung sämtlicher datenschutzrechtlicher Vorgaben. Dabei ist eine saubere Trennung der Verantwortlichkeiten erforderlich, die auch für die Patientinnen und Patienten klar erkennbar sein muss.

Die Patientinnen und Patienten müssen bei jeder Interaktion mit der Website, die sie nutzen, um mit der Praxis einen Termin zu vereinbaren, in der Lage sein, zu erkennen, wer für die jeweilige Datenverarbeitung verantwortlich ist.

Die Verarbeitung von Gesundheitsdaten im Zusammenhang mit einem Nutzerkonto bei einem Terminverwaltungsunternehmen basiert datenschutzrechtlich im Regelfall auf einer Einwilligung.

# Wofür sind Sie verantwortlich?

## MELDEPFLICHT

an Aufsichtsbehörde bei Datenschutzverletzungen gem. **Art. 33 DSGVO**

- Innerhalb von 72 h nachdem die Datenschutzverletzung bekannt wurde
- Online unter: <https://www.datenschutz-mv.de/kontakt/meldung-einer-datenpanne/>
- Meldepflicht **entfällt**, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt (Art. 33 Abs. 1 DS-GVO).  
Abwägung muss dokumentiert werden. **IM ZWEIFEL: MELDEN!**
- ggf. Unterrichtung der betroffenen Personen (Art. 34 DS-GVO)

# Fragen aus Ihrer Praxis



## Der Landesbeauftragte für Datenschutz und Informationsfreiheit

Telefon: 0385 59494-0

E-Mail: [info@datenschutz-mv.de](mailto:info@datenschutz-mv.de)

Internetseite: [www.datenschutz-mv.de](http://www.datenschutz-mv.de)