Zirkeltraining für den Datenschutz - In neun Stationen fit für die DS-GVO

Dorothee Bär, Staatsministerin für Digitales im Kanzleramt, will digitale Champions League spielen. Ein guter Vorsatz – der sicher auch im medizinischen Sektor gilt. Doch die Fußballbegeisterten unter Ihnen werden es wissen: Allein ein schickes Stadion und ein Ball machen noch keinen Meister. Intelligente Spielzüge und gute Vorarbeit sind ebenso notwendig wie grundlegende Kenntnis der Spielregeln. Die Spielregeln zur modernen Datenverarbeitung finden sich in der frisch gedruckten Europäischen Datenschutz-Grundverordnung (DS-GVO). Ab dem 25. Mai 2018 ist sie in allen Mitgliedstaaten der Europäischen Union unmittelbar anzuwendendes Recht. Ganz egal, ob Sie bei der Digitalisierung auf Champions League – Niveau mitspielen wollen oder dann doch eher auf Papierakten setzen: Die nachfolgenden neun Stationen sind als Einsteigertraining zur Vorbereitung auf die DS-GVO gedacht:

1. **Check-up**

Wie bei jedem Training sollte ganz am Anfang ein ausführlicher Check-up stehen. Grob gesagt muss sich jeder, der personenbezogene Daten eigenverantwortlich verarbeitet, klar machen, wer was wie und warum mit diesen Daten tut. Hier ist Teamplay gefragt. Auch wenn die DS-GVO vom Idealbild des allwissenden Verantwortlichen ausgeht, regen wir ein Brainstorming mit Mitarbeiterinnen und Mitarbeitern an. Dieses Vorgehen sensibilisiert zugleich alle Beteiligten für neue Anforderungen im Datenschutz. Machen Sie sich Notizen und bewahren Sie diese gut auf. Sie werden später darauf zurückgreifen. Nachfolgende Fragestellungen sollten insbesondere beantwortet werden:

a) Welche personenbezogenen Daten gibt es in der Praxis? (Gesundheitsdaten von Patienten, personenbezogene Daten von Mitarbeitern etc...)	b) Was machen Sie mit diesen Daten? (Führen Sie Papierakten, speichern Sie Röntgenbilder in der Cloud, nutzen Sie eine webbasierte Anwendung zur Terminvergabe, nehmen Sie an einem Gesundheitsnetzwerk teil etc.)
c) Wie lange bewahren Sie diese Daten/Akten auf? Ab wann geht eine Akte ins Archiv? Wie realisieren Sie, dass eine Akte ins Archiv gehört?	d) Was machen Ihre Mitarbeiter mit den personenbezogenen Daten? Wie viele Mitarbeiter sind es?
e) Wem und warum übermitteln Sie personenbezogene Daten? Übermitteln Sie in Drittländer (z.Bsp. bei Forschungsvorhaben)?	f) Wer hat Zugang zu diesen Daten? (Mitarbeiter, andere Ärzte der Praxisgemeinschaft, externe Dienstleister, Dritte, wie mitbehandelnde Ärzte, Labore etc.). Von wo kann dieser Zugriff stattfinden (Inland, europäisches Ausland, Drittland)?
g) Zu welchem Zweck verarbeiten Sie die personenbezogenen Daten? (nur zu Behandlung oder auch für Forschung, Qualitätssicherung etc...)	h) Welche Maßnahmen zum Datenschutz haben Sie ergriffen? (Verschlüsselung, Passwörter, abschließbare Schränke etc.)
i) Sind Sie als Einzelarzt oder in einer Praxisgemeinschaft tätig? Nehmen Sie an der vertragsärztlichen Versorgung teil?	j) Was sind die für Sie maßgeblichen gesetzlichen Regelungen Ihrer Tätigkeit (SGB V, Regelungen der Kassenärztlichen Vereinigung etc.)

2. **Die grundlegenden Spielregeln**

Eine Rechtsgrundlage für die Verarbeitung von Patientendaten besteht nach Art. 6 Abs. 1 lit b, 9 Abs. 2 lit. h DS-GVO. Gesetzliche Grundlagen (z.Bsp.: Röntgenverordnung) oder zumindest Empfehlungen der Ärztekammer zur Speicherdauer von Patientendaten sollten geprüft werden. Dokumentieren Sie alle Rechtsgrundlagen oder Empfehlungen. Besonders kritisch sollten Sie die Rechtsgrundlagen prüfen, wenn Sie Patientendaten in Drittländer übermitteln oder dort verarbeiten lassen. Hierfür bedarf es einer ausdrücklichen Rechtsgrundlage. Zudem besteht nicht überall ein gesetzliches Berufsgeheimnis. Auch dies kann sich maßgeblich auf die Zulässigkeit der Datenverarbeitung oder die Anforderungen an die Datenverarbeitung auswirken.

3. **Das Spielsystem**

Nach der DS-GVO muss klar sein, wer Verantwortlicher ist. Das ist die Person oder Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung entscheidet. In der Regel ist das die niedergelassene Ärztin oder der niedergelassene Arzt –keinesfalls die Mitarbeiterin oder der Mitarbeiter. Es können auch mehrere Personen gemeinsam verantwortlich sein. Zum Beispiel, wenn sich eine Praxisgemeinschaft eine IT-Infrastruktur teilt, bei Gesundheitsnetzwerken oder bei Forschungsvorhaben. Darüber hinaus gibt es Auftragsverarbeiter. Hierunter sind insbesondere externe Dienstleister zu verstehen, die mit Patientendaten in Berührung kommen können, beispielsweise bei der Wartung der IT-Technik. Wie auch eigene Mitarbeiterinnen und Mitarbeiter dürfen Auftragsverarbeiter die Patientendaten nur auf Weisung des Verantwortlichen verarbeiten. Nehmen Sie sich also Ihre Aufzeichnung aus Station eins noch einmal zur Hand und überprüfen Sie, ob Sie allein oder mit anderen gemeinsam verantwortlich sind. Unterscheiden Sie bei den anderen Beteiligten zwischen eigenen Mitarbeiterinnen und Mitarbeitern sowie Auftragsverarbeitern. Schließlich müssen Sie bei den Aufzeichnungen ergänzen, wer „Empfänger“ ist. Empfänger ist, wem personenbezogene Daten offengelegt werden. Eine Offenlegung kann durch Übermittlung oder die Ermöglichung des Zugriffs auf Daten erfolgen. Empfänger können also eigene Mitarbeiterinnen und

Mitarbeiter, Auftragsverarbeiter und Dritte sein.

4. Klare Anweisungen

Sind die Rollen klar verteilt, gilt es, dies in entsprechenden Vereinbarungen oder Verträgen festzuhalten. Eigene Mitarbeiter sind dazu zu verpflichten, Patientendaten nur auf bzw. im Rahmen von Weisungen zu verarbeiten, und regelmäßig entsprechend zu schulen oder sensibilisieren.
Auftragsverarbeiter dürfen nur auf Grundlage eines speziellen Vertrages tätig werden (vgl. Art. 28 DS-GVO). Ein Formular für diesen Vertrag finden Sie auf unserer Homepage www.datenschutz-mv.de.
Beachten Sie, dass Sie Mitarbeiter und Auftragsverarbeiter darüber hinaus nach § 203 Abs. 4 StGB zur Geheimhaltung verpflichten (§ 203 Abs. 4 StGB).
Gemeinsame Verantwortliche müssen in einer transparenten Vereinbarung festhalten, wer für was verantwortlich ist.

5. Informationen

Die wohl wichtigste Neuerung der DS-GVO besteht in der Verpflichtung, Patienten über die Datenverarbeitung spätestens bei der Datenerhebung zu informieren. Zukünftig sollte den Patienten ein entsprechendes Informationsformular ausgehändigt werden. Die Informationspflicht besteht nur insoweit, als der Patient noch nicht über die Information verfügt, also einmalig beim nächsten Besuch des Patienten und erneut nur dann, wenn sich etwas ändert. Mitarbeiter sollten ausdrücklich darauf hingewiesen werden, die Formulare auszugeben und auch geschult werden, um etwaige Nachfragen beantworten zu können. Im Praxisinformationssystem oder der Patientenakte sollte vermerkt werden, dass das Formular ausgehändigt wurde. Ein Aushang in der Praxis, ein Plakat mit einer graphischen Darstellung oder ein kurzes Video können das Formular zwar nicht ersetzen, aber sinnvoll ergänzen. Ausführliche Hinweise zur Erstellung von Informationsformularen finden Sie ebenfalls auf unserer Homepage.

6. Die Abwehr muss stehen

Ärzte sind verpflichtet, ein Verzeichnis von Verarbeitungstätigkeiten zu führen. In Station eins haben Sie hierfür gut vorgearbeitet. Ein Formular für das Verzeichnis finden Sie auf unserer Homepage. Darüber hinaus können Sie sich im Streitfall entlasten, wenn Sie Maßnahmen zum Datenschutz, wie Schulungen von Mitarbeitern, dokumentieren. Eine besondere Form der Dokumentation verlangt in bestimmten Fällen die Datenschutz-Folgenabschätzung. Eine Datenschutz-Folgenabschätzung kann bei einer umfangreichen Verarbeitung von Gesundheitsdaten erforderlich sein. Verarbeiten in einer Praxis weniger als 10 Personen personenbezogene Daten (Mitarbeiter und Ärzte), wird in der Regel nicht von einer umfangreichen Verarbeitung von Gesundheitsdaten auszugehen sein. Allerdings können auch andere Risikofaktoren, wie beispielsweise die Speicherung von Patientendaten in einer Cloud, die Einbindung von Gesundheitsapps, die Übermittlung von Gesundheitsdaten in Drittstaaten im Rahmen von Forschungsvorhaben oder die Teilnahme an Gesundheitsnetzwerken eine Datenschutz-Folgenabschätzung erforderlich machen. Im Rahmen der gemeinsamen Verantwortlichkeit, beispielsweise bei Netzwerken, besteht allerdings auch die Möglichkeit, dass nur ein Verantwortlicher eine Datenschutz-Folgenabschätzung für alle vornimmt. Eine Datenschutz-Folgenabschätzung kann für bestimmte Produkte auch bereits vorliegen. Mit zuverlässigen Partnern ist mehr Digitalisierung in der Arztpraxis also nicht zwingend mit Mehraufwand durch eine Datenschutz-Folgenabschätzung verbunden.

7. Brauchen wir einen „letzten Mann“?

Nach § 38 BDSG-neu müssen Arztpraxen einen Datenschutzbeauftragten bestellen, wenn insgesamt min.10 Personen personenbezogene Daten verarbeiten oder aber eine Datenschutz-Folgenabschätzung (siehe oben) durchgeführt werden muss. Wenn der „letzte Mann“ im modernen Fußball auch aus der Mode gekommen ist, wer Digitalisierung in der Arztpraxis auf Champions League-Niveau betreiben möchte, ist in jedem Fall gut beraten, dies mit der fachmännischen Unterstützung eines internen oder externen Datenschutzbeauftragten zu tun.

8. Kontrolle der Ausrüstung

Nicht wirklich neu ist das Erfordernis technischer und organisatorischer Maßnahmen zur Datensicherheit, die auch regelmäßig überprüft und ggf. verbessert werden müssen. Insbesondere muss die Datenverarbeitung so gestaltet sein, dass die Betroffenen ihre Rechte wahrnehmen können. So muss beispielsweise die Erteilung einer Auskunft nach Art. 15 DS-GVO, die Berichtigung falscher Daten nach Art. 16 DS-GVO oder die Einschränkung der Verarbeitung nach Art. 18 DS-GVO schnell und problemlos möglich sein. Auch ein Verfahren zur Meldung von Datenpannen muss etabliert werden. Mitarbeiter müssen entsprechend geschult werden.

9. Das Verhältnis zum Schiedsrichter

Grundsätzlich unterliegen auch Berufsgeheimnisträger in M-V der Aufsicht des Landesbeauftragten für

Datenschutz und Informationsfreiheit M-V (LfDI M-V). Auf Verlangen ist dem LfDI M-V Auskunft zu erteilen oder Zugang zur Arztpraxis zu gewähren. Eine Verweigerung kann ein empfindliches Bußgeld nach sich ziehen. Ebenso sind jedenfalls vollziehbare Anordnungen des LfDI M-V umzusetzen. Diese können nicht nur im Verwaltungsverfahren sondern ebenfalls mit Bußgeldern durchgesetzt werden. Auch wenn die DS-GVO hohe Bußgelder vorsieht und nahezu jeder Verstoß gegen eine Bestimmung der DS-GVO bußgeldbewehrt ist, gilt aber auch hier der Grundsatz der Verhältnismäßigkeit. Dem LfDI M-V werden in vielen Fällen auch mildere Mittel als hohe Bußgelder zur Verfügung stehen, eine datenschutzkonforme Datenverarbeitung durchzusetzen. Nicht zuletzt möchten wir mit Beratungen und Schulungen dazu beitragen, dass es zu Datenschutzverstößen erst gar nicht kommt!

Heinz Müller, der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern und Lydia Kämpfe, Referentin beim Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern