Fragen FV der Gesundheitsbetriebe zur DSGVO für folgende Mitgliedsbetriebe:

Selbstständiges Ambulatorium, bettenführende Krankenanstalten, Kuranstalten, Sonderkrankenanstalten, Alten- und Pflegeheime

1. Muss ich bei der Verarbeitung von personenbezogenen Daten wie bspw von Patientendaten, Mitarbeiterdaten, usw stets die Einwilligung der betroffenen Person einholen?

Antwort: Als Verantwortlicher gilt es zu prüfen auf welcher rechtlichen Grundlage die Verarbeitung personenbezogener Daten durchgeführt wird bzw werden kann. Zu unterscheiden ist die Verarbeitung personenbezogener Daten ("normale" Daten) wie Name, Adresse, Geburtsdatum, usw und die Verarbeitung besonderer Kategorien personenbezogener Daten ("sensible" Daten) wie Gesundheitsdaten, genetischen und biometrischen Daten, etc.

Während eine rechtmäßige Verarbeitung "normaler" Daten nicht nur auf Basis einer Einwilligung des Betroffenen, sondern auch im Rahmen der Erfüllung eines Vertrags, aufgrund einer rechtlichen Verpflichtung, zum Schutz lebenswichtiger Interessen, im öffentlichen Interesse bzw in Ausübung öffentlicher Gewalt oder aufgrund eines berechtigten Interessen des Verantwortlichen erfolgen kann, sind die rechtlichen Bedingungen für die Verarbeitung sensibler Daten restriktiver. Die Verarbeitung "sensibler" Daten darf aus Gründen des Arbeits- oder Sozialrechts, einschließlich der Kollektivverträge und Betriebsvereinbarungen, zum Schutz lebenswichtiger Interessen oder aufgrund geeigneter Garantien durch politisch, weltanschaulich, religiös oder gewerkschaftlich ausgerichtete Organisationen erfolgen. Überdies sieht die DGSVO vor, dass "sensible" Daten, die offensichtlich von der betroffenen Person selbst öffentlich gemacht wurden, vom Verantwortlichen verarbeitet werden dürfen. Ebenfalls liegt eine rechtmäßige Verarbeitung sensibler Daten bei der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen. Weiters ist eine Verarbeitung von sensiblen Daten nach den Bestimmungen der DSGVO rechtmäßig, wenn diese aus Gründen eines erheblichen öffentlichen Interesses oder auf im öffentlichen Interesse liegenden Archivzwecken beruht. Zudem können sensible Daten für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke verwendet werden.

Für Gesundheitsbetriebe gilt eine rechtmäßige Verarbeitung auch für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich aufgrund von Gesetzen oder eines Vertrags mit einem Angehörigen eines Gesundheitsberufs. Diesbezüglich dürfen die Daten von Fachpersonal, das einem Berufsgeheimnisses und/oder einer Geheimhaltungspflicht unterliegt, verarbeitet werden. IdZ kann es zu weiteren Bedingungen einschließlich Beschränkungen durch nationale Gesetze, wie bspw durch das Ärztegesetz, kommen. Für den Fall, dass keine der oben

angeführten Rechtsgrundlagen zur Verarbeitung personenbezogener Daten Anwendung findet, ist vom Verantwortlichen eine ausdrückliche Einwilligung der betroffenen Person einzuholen.

Einwilligungen (ausdrückliche sowie "normale") können jederzeit vom Betroffenen mit sofortiger Wirkung widerrufen werden. Dies bedeutet, dass mit Einlagen des Widerrufs die Datenverarbeitung einzustellen wäre und der Betroffene auch über die Auswirkungen seines Widerrufs informiert werden muss. Die Rechtsgrundlage "Einwilligung" ist insofern vom zukünftigen Verhalten des Betroffenen abhängig und ist es aus diesem Grund empfehlenswert, stets zu prüfen, ob sich eine Datenverarbeitung auf eine "stabilere" der zuvor aufgelisteten Rechtsgrundlagen stützen lässt.

2. Befunde und Bilder werden oft nicht von der untersuchten Person abgeholt. Darf ein Gesundheitsbetrieb diese an Dritte aushändigen?

Antwort: Befunde / Bilder gelten nach der DSGVO als personenbezogene Daten und werden aufgrund ihres gesundheitsbezogenen Inhalts regelmäßig unter die besonderen Kategorien personenbezogener Daten iSd Art 9 DSGVO fallen. Das Aushändigen solcher Daten an Dritte kann als eine Datenübermittlung oder, bei entsprechender Art der Anfrage, als eine datenschutzrechtliche Auskunftsbeantwortung qualifizieren (so zB wenn ein Familienmitglied für die untersuchte Person um Herausgabe ansucht). In beiden Fällen wäre aber (mit je unterschiedlicher rechtlicher Begründung) die Identität desjenigen zu prüfen, der die Befunde / Bilder abholt. Die Abholung dieser Unterlagen durch Dritte bedeutet möglicherweise die Offenlegung personenbezogener Gesundheitsdaten an eine vom Patienten verschiedene Person. Hierzu wäre grundsätzlich die Einwilligung des Patienten erforderlich. Zu überlegen wäre, die Einwilligungserklärungen zB in den Aufnahmeformularen, jedoch stets als eigenständige und eindeutig als Einwilligung gekennzeichnete Erklärung, einzuholen. In diesen wäre dann vom Patienten auch zu spezifizieren, wer abholberechtigt ist.

3. Wie ist zu dokumentieren, dass die Person die den Befund oder das Bild (CT/MR/Röntgen) abholt, auch tatsächlich der Patient ist?

Antwort: Man könnte bspw gewisse Identifikationsmerkmale abfragen (Geburtsdatum, Name, Wohnort) oder sich einen Ausweis vorlegen lassen. Für die interne Dokumentation könnte der erfolgte Identitätscheck festgehalten werden, oder etwa eine Kopie des vorgelegten Ausweises intern hinterlegt werden.

4. Dürfen Befunde per Mail an Patienten geschickt werden?

Antwort: Die DSGVO verlangt nach einem dem "Risiko angemessenen" Schutzniveau, und erwähnt hierbei auch die Verschlüsselung. Im Sinne einer Risikoangemessenheit wird man bejahen müssen, dass Befunde per Mail nur in verschlüsselter Form zu versenden sind. Es gilt zu beachten, dass eine Mail aus ihrem eigentlichen Inhalt und den eventuell beigefügten Dateianhängen besteht. Beides kann personenbezogene Daten beinhalten. Bei Gesundheitsdaten (wie Befunden), die als besondere Kategorien von Daten im Sinne des Art 9 DSGVO einem erweiterten Schutzbereich unterliegen, sollte man die Verschlüsselung der E-Mail und ihrer Anhänge zumindest in Erwägung ziehen.

In diese Richtung geht auch die Wertung des österreichischen Gesetzgebers, zum Ausdruck gebracht durch das GTelG. Ebenfalls vertrat zB kürzlich der Sächsische Landesdatenschutzbeauftragte die

Auffassung, dass zumindest Berufsgeheimnisträger Mails zu verschlüsseln haben, wenn diese besondere Kategorien von Daten beinhalten (dies allerdings unter starker Bezugnahme auf das BDSG): https://www.saechsdsb.de/images/stories/sdb_inhalt/noeb/taetigkeitsberichte/8-TB-Endfassung-Version-5.pdf

Die Datenschutzbehörde selbst hat bislang noch keine definitive Aussage bzgl E-Mail-Verschlüsselung getroffen, hat jedoch in einem Bescheid zu einem Gesundheitszentrum ausgewiesen, dass in der DSGVO eine unmittelbare oder mittelbare Verpflichtung zur E-Mailverschlüsselung nicht ableitbar wäre (DSB-D213.692/0001-DSB/2018 vom 16.11.2018).

De facto scheitert die Verwirklichung dieser Vorgabe oft an dem Umstand, dass der Patient nicht in der Lage (oder Willens) ist, mit Verschlüsselungsmaßnahmen umzugehen. In der Praxis behilft man sich aktuell damit, den Patienten vorab über die Unsicherheiten unverschlüsselter E-Mailübertragung aufzuklären und dann die Einwilligung zur unverschlüsselten Mailversendung einzuholen, dem wurde allerdings von der Datenschutzbehörde eine Abfuhr erteilt. Mehr und mehr kommen daher sichere Lösungen auf, die die E-Mailübertragung ausblenden und den datenschutzrechtlich geforderten technischen und organisatorischen Maßnahmen entsprechen. So etwa die Bereitstellung eines Zugangscodes für die Homepage, auf welcher in einem geschützten Bereich die Befunde hinterlegt sind und auf welche der Patient direkt zugreifen und die Befunde herunterladen kann.

5. Dürfen personenbezogene Daten elektronisch an SV-Träger übermittelt werden?

Antwort: Grundsätzlich dürfen personenbezogene Daten an SV-Träger übermittelt werden, sofern hierfür unter der DSGVO eine Berechtigung besteht (etwa wenn dies für die Abrechnungszwecke des SV-Trägers notwendig ist). Zur Sicherheitsthematik der Versendung personenbezogener Gesundheitsdaten siehe oben. Wichtig ist, dass auch Datenübermittlungen an SV-Träger dem datenschutzrechtlichen Verhältnismäßigkeitsprinzip unterliegen. Das bedeutet, auch Datenübermittlungen an SV-Träger dürfen nur im absolut notwendigen Ausmaß, sofern also etwa für die Abrechnungsbelange notwendig, erfolgen.

6. Dürfen Befunde bzw. personenbezogene Daten per Mail an andere Ärzte und Krankenanstalten geschickt werden?

Antwort: Hinsichtlich der Verwendung von Gesundheitsdaten siehe oben. Hinsichtlich des Datenaustauschs unter Gesundheitsdiensteanbietern (zB Ärzten, Krankenanstalten) sind zusätzlich die Vorgaben des GTelG zu beachten. Überdies ist festzuhalten, dass die DSGVO keine Privilegierung für Datenübermittlungen innerhalb von Berufsgruppen vorsieht. Dies bedeutet, dass jede Datenübermittlung zuvor auf deren Einklang mit der DSGVO zu prüfen ist, auch wenn sie innerhalb einer Berufsgruppe (hier: zwischen Gesundheitsdiensteanbietern) stattfindet.

7. Dürfen Befunde bzw. personenbezogene Daten per Fax (Faxerkennung ist vorhanden) an andere Ärzte geschickt werden?

Antwort: Das GTelG enthält in seiner aktuellen Fassung Übergangsbestimmungen, die die Weitergabe von Gesundheitsdaten per Fax erlauben, sofern keine geeignete technische Infrastruktur zur sicheren Weitergabe der Daten vorhanden ist bzw wenn keine zumutbaren und wirtschaftlich vertretbaren

Mittel zur sicheren elektronischen Datenweitergabe vorhanden sind. Das Gesetz ist also bestückt mit unbestimmten Gesetzesbegriffen, die Einzelfallprüfungen leider unumgänglich machen. Selbst wenn man sich aber auf diese "erleichterten Bedingungen" des GTelG beruft, sind die im GTelG vorgesehenen gegenseitigen Verifizierungsmaßnahmen desjenigen, der das Fax versendet und desjenigen, der das Fax erhält, sowie die Sicherheitseinstellungen am Fax zu wahren.

8. Dürfen Befunde auf einen Server hochgeladen werden und der Patient holt sich diese mit einem TAN, welchen er zuvor seitens des Ambulatoriums erhalten hat?

Antwort: Siehe oben. Dies könnte sogar als besser gesicherter Übertragungsweg qualifizieren, als dies bei E-Mails der Fall wäre. Wird der Server bzw das Downloadportal von einem Dritten betrieben, so müsste hierzu ein DSGVO-konformes Setup erstellt werden. Typischer Weise könnte der Dritte als ein Auftragsverarbeiter qualifiziert werden, mit dem ein Vertrag gem Art 28 DSGVO zu schließen wäre. Wird die Plattformlösung im EU-Ausland betrieben, so müssten zusätzlich noch Schritte unter der DSGVO ergriffen werden, um die Wahrung des europäischen Datenschutzniveaus sicherzustellen (etwa durch eine "Privacy Shield"-Zertifizierung falls der Plattformbetreiber ein US-Unternehmen ist).

9. Übermittlung von Impfdaten von Kindern an Gemeinden – ist das zulässig? Wenn ja, in welcher Form darf die Übermittlung erfolgen?

Antwort: Jede Datenübermittlung, auch von Impfdaten, bedarf einer rechtlichen Grundlage, zB aufgrund gesetzlichen Auftrags oder aufgrund von Einwilligung (bei Kindern: des Erziehungsberechtigten). Wenn jedoch eine entsprechende rechtliche Grundlage für die Datenübermittlung an die Gemeinden besteht, kann darauf auch die Übermittlung von Impfdaten gestützt werden. Eine gesonderte Einwilligung wäre in diesem Fall nicht erforderlich.

10. Dürfen Daten von Kindern an jeden Elternteil ausgehändigt werden, oder muss das Sorgerecht überprüft werden?

Antwort: Sofern nicht Zweifel an der Obsorgeberechtigung des anfragenden Elternteils bestehen, darf grundsätzlich von der Berechtigung des Elternteils zum Datenerhalt ausgegangen werden. Dies ergibt sich sinngemäß aus der "Zweifelsregel" des Art 12 Abs 6 DSGVO, wonach bei begründeten Zweifel an der Identität der anfragenden Person weitere Informationen eingeholt werden können. Ebenso können weitere Informationen erfragt werden, wenn sich begründete Zweifel an der Obsorgeberechtigung des anfragenden Elternteils ergeben.

11. Wie ist innerbetrieblich mir personenbezogenen Daten umzugehen? Darf jeder Mitarbeiter Zugang zu diesen haben?

Antwort: Mitarbeiter dürfen nur in jenem Ausmaß Datenzugriff haben, als die Mitarbeiter für ihre jeweilige Aufgabenerfüllung und im Rahmen ihrer jeweiligen Zuständigkeiten diese Daten tatsächlich benötigen. Zugriffe "einfach nur so", oder ohne sonst eine rechtfertigbare Notwendigkeit, wären unter der DSGVO nicht zulässig. Um sicherzustellen, dass ausschließlich jene Mitarbeiter Zugriff auf personenbezogene Daten haben, die diese Daten tatsächlich zur Erfüllung ihrer arbeitsvertraglich

geschuldeten Pflicht benötigen, sind geeignete technische und organisatorische Maßnahmen umzusetzen. Unter einer technischen Maßnahme wäre bspw die Einführung von Rollenverteilungen im elektronischen System zu verstehen. Ausgehend von der Notwendigkeit des konkreten Datenbedarfs durch den Mitarbeiter sind diesem unterschiedliche Zugriffsrechte zu gewähren. Zusätzlich sind geeignete organisatorische Maßnahmen, etwa in Form von Dienstanweisungen, zu treffen.

12. Muss im Verfahrensverzeichnis jede Auswertung gesondert aufgelistet werden oder reicht eine Auflistung der verarbeiteten Datenkategorien?

Antwort: Der Verantwortliche muss schriftlich ein Verzeichnis aller Verarbeitungstätigkeiten (=Datenanwendungen), die seiner Zuständigkeit unterliegen, führen. Eine Vorschrift zur "Verzeichnistiefe" findet sich in der DSGVO nicht Dieses Verzeichnis hat jedenfalls zu enthalten: den Namen und die Kontaktdaten des Verantwortlichen, Daten seines Vertreters (falls vorhanden), Daten des Datenschutzbeauftragten (falls bestellt), die Zwecke der Verarbeitung, die Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten, Kategorien von Empfängern (einschließlich Empfänger in Drittländern oder internationalen Organisationen); wenn möglich: Löschungsfristen sowie eine Beschreibung der technischen und organisatorischen Maßnahmen. Damit statuiert die DSGVO grundsätzlich die Pflicht zur kategorisierenden Beschreibung. Einzelne Auswertungsdaten, oder ähnliches, müssen im Verzeichnis nicht angeführt werden.

13. Sowohl steuerrechtlich als auch laut Ärztegesetz besteht eine Aufbewahrungspflicht, wie ist diese im Sinne der DSGVO umzusetzen?

Antwort: Die DSGVO selbst normiert keine Aufbewahrungsfristen. Allerdings ergibt sich aus dem datenschutzrechtlichen Grundsatz der Speicherbegrenzung, dass die Aufbewahrung personenbezogener Daten auf das unbedingt erforderliche Mindestmaß beschränkt zu bleiben hat. Hier spielen die rechtlichen Aufbewahrungsfristen der jeweils anzuwendenden Materiegesetze hinein. Solange es gesetzliche Aufbewahrungspflichten zu beachten gilt, welche die Aufbewahrung der Daten erfordern (oder diese auch zur Erfüllung des Behandlungsvertrages notwendig sind) dürfen bzw müssen die Daten aufbewahrt werden.

Die zur Anwendung kommenden Aufbewahrungsfristen sind oft vielschichtig. Steuerrechtliche Aufbewahrungsfristen ergeben andere Aufbewahrungsfristen als etwa jene des Ärztegesetzes. Um diesen Differenzierungen gerecht zu werden, muss ein Löschkonzept ins Leben gerufen werden. Gemäß diesem Konzept wären die Patientendaten zu unterteilen, sodass etwa die buchhaltungsrelevanten Informationen getrennt von den medizinisch relevanten Informationen erfasst und gesonderten Löschroutinen unterstellt werden. Bei derartigen Umsetzungen handelt es sich in der Praxis um eine der schwierigsten Aufgaben der DSGVO-Compliance.

Ein einseitig gestaltbares Recht des Verantwortlichen, eine für ihn "günstigere" Frist zu wählen, besteht aber nicht. Vielmehr ergibt sich aus in objektiver Weise aus dem Inhalt des Datums, welche Aufbewahrungsfrist zur Anwendung kommt.

14. Müssen Daten von Verstorbenen gelöscht werden? Wann und wie hat die Löschung zu erfolgen?

Antwort: Prinzipiell erlöschen alle Grundrechte mit dem Tod, also auch das Recht auf Datenschutz. Auch wird in den Erwägungsgründen der DSGVO dargelegt, dass die DSGVO nicht für personenbezogenen Daten Verstorbener gilt. Bei der Verwendung dieser Daten ist jedoch darauf zu achten, dass das informationelle Selbstbestimmungsrecht von Lebenden nicht verletzt wird (bspw könnte durch Verarbeiten der Krankheit an der jemand gestorben ist, ein Rückschluss auf Angehörige getroffen werden). Es sind insbesondere auch Berufsgeheimnisse, ua die ärztliche Schweigepflicht, zu wahren. Um kein unnötiges Risiko einzugehen, empfiehlt es sich auch die Daten von Verstorbenen zu löschen, sofern deren Aufbewahrung nicht mehr sachlich gerechtfertigt ist (also zB wenn gesetzliche Aufbewahrungsfristen abgelaufen sind). Dienen diese Daten aber bspw als potentielle Beweismittel, so sind sie weiter aufzubewahren. Wenn also daher zB Hinterbliebene einen Schadenersatzprozess gegen ein Krankenhaus anstreben, könnten Daten zur Behandlung des Verstorbenen für dieses Verfahren Beweismittelcharakter haben, was deren Aufbewahrung rechtfertigen würde. Somit ist von der Löschung der Daten Verstorbener bei der Erfüllung gesetzlicher Verpflichtungen sowie behördlicher Anweisungen bzw. gerichtlicher Strafverfahren abzusehen. Die Aufbewahrung der Daten sollte wie bereits an obiger Stelle erwähnt nur bis zur Erreichung des konkreten Zwecks ihrer Aufbewahrung werden.

15. Worin liegt datenschutzrechtlich die Unterscheidung, wenn ein Patient mit einer Zuweisung zu einem Arzt geht oder ohne von Arzt zu Arzt geschickt wird?

Antwort: Datenschutzrechtlich ist diese Unterscheidung von keiner primären Relevanz. Jeder Arzt darf / muss im Rahmen seiner Berufsbefugnis Patientendaten verarbeiten. Ob der Patient zu einem Arzt aufgrund einer Überweisung geschickt wird oder ob er aus eigenen Stücken den Arzt aufsucht, ist unter der DSGVO kein maßgebliches Unterscheidungskriterium. Hiervon gesondert zu beurteilen ist die Zulässigkeit einer allfälligen Datenübermittlung der Ärzte untereinander. Bei dieser sind stets die gesetzlichen Vorgaben, etwa des Ärztegesetzes oder des Gesundheitstelematikgesetzes, zu berücksichtigen.

16. Dürfen personenbezogene Daten welche aufgrund des Patienten-Arzt Verhältnisses vorliegen, auch für Informationsschreiben an Patienten genutzt werden?

Antwort: Die ärztliche Verschwiegenheitspflicht gilt nicht gegenüber dem eigenen Patienten. Aus datenschutzrechtlicher Sicht kann der Patient für notwendige bzw aus ärztlicher Sorgfaltspflicht geschuldete Informationen kontaktiert werden und es dürfen die Kontaktdaten des Patienten verwendet werden. Möchte der Arzt aber zB elektronische Werbemaßnahmen durchführen, oder ähnliches, und dazu die Kontaktdaten seiner Patienten verwenden, so bedürfte er dafür der Zustimmung der Patienten.

17. Übernimmt ein Datenschutzbeauftragter die Haftung?

Antwort: Die Bestellung eines Datenschutzbeauftragten befreit den Verantwortlichen nicht davor, die Verpflichtungen der DSGVO einzuhalten. Eine mögliche Bestellung eines Datenschutzbeauftragten auch als "verantwortlicher Beauftragter" nach dem Verwaltungsstrafgesetz und sohin als potentieller Strafadressat wird nach Ansicht der Datenschutzbehörde abgelehnt. Hierbei führt die Datenschutzbehörde aus, dass der Datenschutzbeauftragte eine beratende Funktion hat. Verbindliche Anordnungen sind von der Managementebene zu treffen. Zur Parallelbestellung des

Datenschutzbeauftragten auch zum "Verantwortlichen Beauftragten" im Sinne des § 9 VStG werden Bedenken hinsichtlich eines möglichen Interessenkonflikts in der Person des Bestellten gesehen, welcher einer solchen Parallelbestellung entgegenstehen könnte. Hierbei handelt es sich aber bislang "bloß" um eine abstrakte Diskussion. Es bestehen durchaus gegenteilige Argumente Durch behördliche oder gerichtliche Entscheidung wurde die Frage der Parallelbestellung bis dato nicht geklärt.

18. Ab wie viel Vollzeitäquivalenten ist ein Datenschutzbeauftragter notwendig?

Antwort: Die Bestellung eines Datenschutzbeauftragten ist nach der DSGVO nicht abhängig von der Anzahl an Mitarbeitern im Unternehmen bzw der Einrichtung. Die DSGVO verpflichtet einen Verantwortlichen zur Bestellung eines Datenschutzbeauftragten in den folgenden Fällen (sinngemäßes gilt auch für Auftragsverarbeiter):

- Wenn es sich beim Verantwortlichen um eine Behörde oder öffentliche Stelle handelt;
- Wenn es die Kerntätigkeit des Verantwortlichen ist, umfangreiche regelmäßige systematische Überwachungen von Betroffenen vorzunehmen;
- Wenn es Kerntätigkeit des Verantwortlichen ist, umfangreich besondere Kategorien von Daten (etwa Gesundheitsdaten) zu verarbeiten.

Überdies ermächtigt die DSGVO die EU-Mitgliedsstaaten, über die obige Auflistung hinaus in sonstigen Fällen die Benennung von Datenschutzbeauftragten vorzuschreiben, wovon ua der deutsche Gesetzgeber Gebrauch gemacht hat (in Deutschland kannte man den betrieblichen Datenschutzbeauftragten bereits vor der DSGVO; insofern hat man die Verpflichtungen zur Bestellung beibehalten). Nach dem deutschen Bundesdatenschutzgesetz besteht eine Pflicht zur Benennung auch ab zehn Personen, die ständig mit der automatisierten Datenverarbeitung beschäftigt sind. Trotz Nichtvorhandenseins einer solchen Bestimmung im österreichischen Datenschutzgesetz, ist aufgrund der vergleichbaren Rechtssysteme – und unter Verweis auf Aussendungen der Ärztekammer zum Thema Datenschutzgrundverordnung – in Gruppenpraxen in denen mehr als zehn Mitarbeiter (Vollzeitäquivalente) Zugriff auf personenbezogene Patientendaten haben, die Bestellung eines Datenschutzbeauftragten zu empfehlen. Unter dem Begriff der Kerntätigkeit ist jene Tätigkeit zu verstehen, die der Verwirklichung der Ziele der Verantwortlichen dient. Die Kerntätigkeit von Krankenhäusern liegt in der Erbringung von Gesundheitsdienstleistungen, was die Verarbeitung personenbezogener Patientendaten und sonstiger damit zusammenhängender Gesundheitsdaten bedingt. Daher werden diese Datenverarbeitungen als Teil der Kerntätigkeit von Krankenhäusern erachtetet und aufgrund des Umfangs der Verarbeitung besonderer Datenkategorien (Gesundheitsdaten) wird die Pflicht des Krankenhauses zur Bestellung eines Datenschutzbeauftragten abgeleitet (vgl WP 243 der Art 29 Datenschutzgruppe).

Nach einem jüngeren Bescheid der Datenschutzbehörde (DSB-D213.692/0001-DSB/2018 vom 16.11.2018) wurde im Falle eines Allergiezentrums eine Kerntätigkeit in der Diagnostik und Behandlung (Verarbeitung von Gesundheitsdaten) gesehen und im Falle von 17 Ärzten + 14 weiteren tlw auch mit Datenverarbeitung befassten Mitarbeitern + Aufbewahrungsdauer von 10 Jahren (aufgrund von § 51 ÄrzteG) eine umfangreiche Verarbeitung bejaht, weshalb ein Datenschutzbeauftragter nach Ansicht der Datenschutzbehörde zu bestellen war.

Nach wie vor gilt eine Abwägung im Einzelfall. In Fällen, in denen die DSGVO die Bestellung eines DSB nicht ausdrücklich normiert, können es Verantwortliche mitunter als zweckmäßig erachten, einen solchen auf freiwilliger Basis zu bestellen.

19. Wann ist eine Datenschutz-Folgeabschätzung zu erstellen?

Antwort: Eine Datenschutz-Folgenabschätzung ist ein Verfahren zur Sicherstellung und zum Nachweis der Einhaltung der datenschutzrechtlichen Anforderungen. Sie ist erforderlich, wenn die Verarbeitung personenbezogener Daten wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringt. Die DSGVO sieht dies (unter anderem) dann als erfüllt an, wenn umfangreiche Verarbeitungen besonderer Datenkategorien (etwa Gesundheitsdaten) vorgenommen werden. Ebenso bei umfassenden Bewertung und Auswertungen von Personen (etwa Profiling) oder bei der Überwachung öffentlicher Bereiche. Beispielhaft für den Bedarf an einer Datenschutz-Folgenabschätzung kann ein Krankenhaus genannt werden, das medizinische Daten seiner Patienten in großem Umfang verarbeitet. Die Verarbeitung personenbezogener Patientendaten durch einen einzelnen Arzt löst hingegen keine Pflicht einer Datenschutzfolgeabschätzung aus (beides entnehmbar dem WP 248 der Art 29 Datenschutzgruppe).

Grundsätzlich ist eine Datenschutz-Folgenabschätzung vorab, dh vor Aufnahme der betreffenden Verarbeitungstätigkeiten durchzuführen. Aber auch für bereits laufende Verarbeitungsvorgänge ist eine solche Folgenabschätzung durch den Verantwortlichen vorzunehmen. In Fällen, in denen eine mit hohen Risiken verbundene Datenverarbeitung geplant ist oder bereits durchgeführt wird, stellt die Datenschutz-Folgenabschätzung ein zentrales Element bei der Einhaltung der DSGVO dar.

Die DSGVO erlaubt der Aufsichtsbehörde (Österreich: Datenschutzbehörde) durch Verordnung jene Datenverarbeitungen festzuschreiben, in denen keinesfalls eine Datenschutz-Folgenabschätzung erforderlich ist ("Whitelist") und in denen jedenfalls eine Datenschutz-Folgenabschätzung durchzuführen ist ("Blacklist"). Eine "Whitelist" wurde bereits erlassen. Diese befreit (unter anderem) die Patienten-/Klienten-/Kundenverwaltung und Honorarabrechnung einzelner Ärzte, Gesundheitsdiensteanbieter und Apotheken von der Pflicht zur Datenschutz-Folgenabschätzung, da in diesem Fall wohl nicht von einer „umfangreichen“ Verarbeitung ausgegangen wird (vgl auch die Bestellung eines Datenschutzbeauftragten). Die "Blacklist" adressiert Krankenanstalten oder Ärzte nicht explizit, sieht aber die Pflicht zur Datenschutz-Folgenabschätzung in generellen Szenarien vor, die auch für Gesundheitsdiensteanbieter von Relevanz sind (etwa Verarbeitung besonderer Datenkategorien im hohen Umfang, wenn es sich dabei um Patienten als Betroffene handelt). Achtung: Zwischen der Anwendung der Whitelist („einzelne Ärzte“) und der „Blacklist“ (umfangreiche Verarbeitung sensibler Daten von Patienten) liegt ein sehr großer Raum, der im Einzelfall geprüft werden muss. Wichtig ist bei der Datenschutz-Folgenabschätzung: Prüfen, ob eine nach den jetzigen Vorschriften zwingend vorgenommen werden muss und begründen, wenn angenommen wird, dass keine durchgeführt werden muss! Im Zweifelsfall ist - nicht zuletzt auch aus Haftungsgründen – eine Datenschutz-Folgenabschätzung zu erstellen (WP 248 der Art 29 Datenschutzgruppe).

20. Wie haben Datensicherheitsmaßnahmen gemäß DSGVO zu erfolgen?

Antwort: Grundsätzlich ist zwischen Datenschutz und Datensicherheit zu differenzieren. Das Thema der Datensicherheit hat in der DSGVO einen wesentlichen Stellenwert eingenommen, weshalb hier aufgrund des Umfanges nur die wichtigsten Punkte angeführt werden können. Die Einführung geeigneter technischer und organisatorischer Maßnahmen durch den Verantwortlichen lässt sich schon aus dem Grundsatz der Integrität und Vertraulichkeit ableiten. Die genannten Sicherheitsmaßnahmen sind stets unter Berücksichtigung des Standes der Technik zu adaptieren. Unter technischen und organisatorischen Maßnahmen werden allgemein Pseudonymisierung und Verschlüsselung von personenbezogenen Daten, die korrekte Funktionsfähigkeit von Systemen und Diensten, die

Wiederherstellbarkeit von Daten nach einem physischen oder technischen Zwischenfall, sowie die regelmäßige Überprüfung der sicheren Verarbeitung von personenbezogenen Daten verstanden.

Neben den technischen und organisatorischen Maßnahmen empfiehlt sich der Aufbau eines Informationssicherheitsmanagementsystems, welches zur Gewährleistung einer umfassenden und nachhaltigen Informationssicherheit unerlässlich erscheint. Ein derartiges System bedarf einer Informationssicherheitspolitik im Unternehmen, welche va sicherheitsrelevante Ziele und Strategien sowie Verantwortlichkeiten und Maßnahmen festlegt.

Überdies ist eine Ermittlung und Bewertung bestehender Sicherheitsrisiken für den Fall einer Störung des IT-Systems vorzunehmen. Verbunden mit einer solchen Risikoanalyse und der Bestimmung der Wahrscheinlichkeit eines Schadeneintrittes sollte eine Risikobewertung unter Bezugnahme der Kosten eines möglichen Schadeneintrittes ausgearbeitet werden.

Ein wesentlicher Bestandteil eines Informationssicherheitsmanagement-systems ist die Ausarbeitung und das Abhalten von regelmäßigen System- und Prozessanhörungen durch interne sowie externe Spezialisten.

Ein weiterer wichtiger Bestandteil eines funktionierenden datenschutzrechtlichen Sicherheitssystems ist die Schulung und Fortbildung von Mitarbeitern in Fragen der Informationssicherheit. Hierbei sollten Mitarbeiter für das Thema Datensicherheit nicht nur sensibilisiert werden, sondern vielmehr sollte ein eigenverantwortliches Bewusstsein für mehr Sicherheit im Umgang mit IT-basierten Systemen geschaffen werden.

21. Sind bei der Befundübermittlung bzw /-anforderung von Proben zwischen selbstständigen Ambulatorien und Ärzten datenschutzrechtliche Erfordernisse zu berücksichtigen? Ergeben sich hierbei Unterschiede, ob der Arzt seine Patienten über die Weiterleitung der Probe zur Befundung informiert oder nicht?

Antwort: Inwieweit bzw ob es überhaupt einen Unterschied macht, dass ein behandelnder Arzt seine Patienten über die Weiterleitung von Proben informiert, hat der OGH ua in seiner Entscheidung (1 Ob 161/16 g) über schadenersatzrechtliche Ansprüche einer Patientin bereits entschieden. Der OGH hielt in der genannten Entscheidung fest, dass ein Arzt – mangels einschränkender Hinweise im Behandlungsvertrag – auch für Fehler des von ihm als Erfüllungsgehilfen beigezogenen Arztes bzw Ambulatoriums einzustehen hat.

Aus datenschutzrechtlicher Sicht muss ungeachtet einer allfälligen (zivilrechtlichen) Erfüllungsgehilfenqualifikation die Legitimation des Datentransfers an das Ambulatorium geprüft werden. Hier ist zunächst zu unterscheiden, ob das Ambulatorium die Proben überhaupt auf personenbezogener Basis (dh unter namentlicher Nennung des Patienten) erhalten muss. Wenn zB dem Arzt oder dem Krankenhaus gegenüber fakturiert wird, so könnte unter Umständen mit einer bloßen numerischen Zuordnung der Probe (oder ähnlichem) das Auslangen gefunden werden (wobei hierzu stets im Detail zu prüfen wäre, ob einer bloß pseudonymisierten Probenübermittlung nicht gesetzliche Dokumentationspflichten des Ambulatoriums entgegenstehen könnten).

Werden die Proben auf personenbezogener Basis (dh, unter namentlicher Nennung des Patienten) weitergegeben, weil dies etwa notwendig ist damit das Ambulatorium direkt gegenüber dem Patienten fakturieren kann oder weil dies aus gesetzlichen Dokumentationspflichten ableitbar ist, so würde die Rechtfertigung für diese Weitergabe der Patientendaten in Art 9 Abs 2 lit h DSGVO liegen, welcher die Verarbeitung von Gesundheitsdaten (unter anderem) für die medizinische Diagnostik und zur Versorgung und Behandlung im Gesundheitsbereich erlaubt. Jedoch sieht § 51 Abs 2 ÄrzteG vor, dass personenbezogene Daten an medizinische Einrichtungen, in deren Behandlung der Kranke steht,

nur mit dessen Einwilligung übermittelt werden dürfen. Qualifiziert man das Ambulatorium als medizinische Einrichtung im gesagten Sinn, so bedürfte der personenbezogene Probentransfer an das Ambulatorium der Einwilligung des Patienten. Diese Einwilligung ist vor Übermittlung an das zuständige Ambulatorium durch den behandelnden Arzt einzuholen. Zur Nachweisbarkeit sollte die Einwilligung schriftlich erfolgen, nicht zuletzt auch deshalb, um den Ambulatorien im Bedarfsfall oder auf Anforderung die erforderliche Einwilligung nachweisen zu können.

Von der Frage der Einwilligung zu unterscheiden ist die Frage, ob der Arzt über den Datentransfer an das Ambulatorium informieren muss. Gem § 3b Abs 2 ÄrzteG wurden die Ärzte von der Pflicht zur datenschutzrechtlichen Information befreit. Im Ergebnis bedeutet dies, dass Ärzte zwar nicht in allgemeiner Form unter der DSGVO über ihre Datenverarbeitungen informieren müssen, wohl aber müssen sie gem § 51 Abs 2 ÄrzteG die Einwilligung des Patienten einholen, wenn sie dessen Daten an andere Ärzte oder Gesundheitseinrichtungen weitergeben.

Alleine die obigen Ausführungen zeigen, dass hier komplexe rechtliche Fragestellungen aufeinandertreffen. Aus der Sicht der Ambulatorien bedeutet dies, dass diese (neben den allgemeinen DSGVO-Pflichten, wie zB jener zur Verzeichnisführung oder zur DSGVO-konformen Information) für sich selbst im Sinne des datenschutzrechtlichen Verhältnismäßigkeitsprinzips beurteilen müssen, ob sie die ihnen übersandten Proben tatsächlich auf personenbezogener (= patientenbezogener) Basis benötigen. Bejahendenfalls darf darauf vertraut werden, dass der Arzt in Entsprechung der ihn gem § 51 Abs 2 ÄrzteG treffenden Pflicht die Einwilligung der Patienten für den Datentransfer an das Ambulatorium eingeholt hat. Sofern sich hieran allerdings Zweifel ergeben, wäre mit dem Arzt eine diesbezügliche Rücksprache zu halten um diesen auf die Bestimmungen des ÄrzteG iZm der Einholung der Einwilligung zu verweisen bzw aufmerksam zu machen.

22. Wenn mit anderen Ärzten Daten ausgetauscht werden bzw. konkret Daten von den Patienten verarbeitet werden, wird dann ein Datenverarbeitungsvertrag benötigt?

Antwort: Wenn Ärzte untereinander Daten "austauschen" dann bedarf dies (neben der Entbindung von der ärztlichen Schweigepflicht) nach einer DSGVO-konformen Rechtfertigung. Diese könnte etwa in der Einwilligung des Patienten zum Datenaustausch liegen. Gerade in Gruppenpraxen könnte auch eine gemeinsame Datenverarbeitung der Ärzte im Sinne des Art 26 DSGVO bestehen. Hierfür bedürfte es eines Vertrags zur Gemeinsamen Datenverarbeitung, welcher den Anforderungen des Art 26 DSGVO entspricht. Dabei gilt es viele Sonderthemen zu berücksichtigen. So entstünde hierbei eine Solidarschuld der teilnehmenden Ärzte. Auch wird gemäß dem aktuellen Entwurf der "Blacklist" für Art 26 Datenverarbeitungen eine spezifische Datenschutz-Folgenabschätzung gefordert.

23. Es gibt Vertreter die Befundungen auf Werkvertragsbasis übernehmen, somit arbeiten sie im System des Ambulatoriums (haben Zugriff auf alle Daten). Sind diese Personen wie Auftragsverarbeiter oder wie unselbstständige Mitarbeiter zu behandeln.

Antwort: Auf Werkvertragsbasis tätige Dritte könnten unter der DSGVO als Auftragsverarbeiter qualifizieren, was den Bedarf einer Vereinbarung nach Art 28 DSGVO auslösen würde. Sind diese Dritte aber derart stark in das Organisationsgefüge des Ambulatoriums eingefügt, dass sie keine gesonderte datenschutzrechtliche Dienstleisterposition erlangen, so wäre ihr Handeln datenschutzrechtlich dem Ambulatoriumsbetreiber (als Verantwortlichen) zuzurechnen. In jedem Fall sollte mit den Dritten eine vertragliche Vereinbarung geschlossen werden, entweder in Ergänzung zum Werkvertrag oder als gesonderte Art 28 DSGVO-Vereinbarung. Denn einer der Hauptnutzen dieser vertraglichen

Zusatzvereinbarung liegt gerade in der Klärung der Frage, welche datenschutzrechtliche Rolle der Dritte im Verhältnis zum Ambulatorium einnimmt. Durch den Vertrag wird zu dieser Frage zwischen den Parteien ein einvernehmliches Verständnis herbeigeführt, und nicht erst im Anlassfall (etwa: Beschwerdefall) erstmals diskutiert.

Fachverband der Gesundheitsbetriebe

Wirtschaftskammer Österreich | Wiedner Hauptstraße 63 | 1045 Wien |
T 05 90 900 – 4980 | F 05 90 900 – 3526
E gesundheitsbetriebe@wko.at | W http://www.gesundheitsbetriebe.at

Stand 26.03.2019