HEIME & SPITÄLER

03
AUGUST
2021

FACHMEDIUM FÜR MANAGEMENT, E-HEALTH, EINKAUF, FOOD, HAUSTECHNIK, IT & PFLEGE

INTERVIEW
08 | Bilanz eines Prozess-Experten

TARDOC
14 | Wie Berset gezielt Tarifpartner schwächt

BAUPLANUNG
34 | Virtuelle Lösung spart Millionen Franken



DATENSCHUTZ & ORGANHAFTUNG

Was Gesundheitsmanager wissen müssen | **20**

careum

Careum
Weiterbildung

Mit Leidenschaft für mehr Lebensqualität

JETZT ANMELDEN

Die Weiterbildung als Care Gastronom/-in startet im November 2021

careum-weiterbildung.ch

Patientendaten in die Cloud? Ja, aber gewusst wie!

Mit der zunehmenden Digitalisierung wurden datenschutzrechtliche Belange zu einem vorrangigen Thema für Institutionen des Gesundheitswesens. Die Auslagerung von Datenbearbeitungen in die Cloud wirft eine Reihe von Rechtsfragen auf, deren Beantwortung anspruchsvoll sein kann. Dieser Beitrag widmet sich zunächst der Frage, welches Datenschutzrecht auf Datenbearbeitungen von Spitälern und Pflegeheimen zur Anwendung kommt, bevor auf ausgewählte Aspekte des Cloud-Computings eingegangen wird.

▶ DR. IUR. MARTIN ZOBL
DR. IUR. CHRISTINE SCHWEIKARD

Welches Datenschutzrecht gilt für wen und was?

Regelungen zum Datenschutz finden sich sowohl auf eidgenössischer als auch auf kantonaler Ebene. Das Bundesgesetz über den Datenschutz (DSG) kommt auf Privatpersonen und Bundesbehörden zur Anwendung; die kantonalen Datenschutzgesetze gelten nur für kantonale öffentliche Organe. Die Europäische Datenschutzgrundverordnung (DSGVO) dürfte in den meisten Fällen nicht zur Anwendung kommen.

Die Unterscheidung hat praktische Konsequenzen: Die auf Privatpersonen anwendbaren Bestimmungen des DSG sind vorwiegend zivilrechtlicher Natur; ihre Verletzung kann vor Zivilgerichten eingeklagt werden. Demgegenüber ist das kantonale Datenschutzrecht öffentlich-rechtlicher Natur; betroffene Personen können sich auf dem verwaltungsrechtlichen Weg zur Wehr setzen. Im Bereich des kantonalen Datenschutzrechts unterstehen die entsprechenden Organisationen zudem der Aufsicht der kantonalen Datenschutzbehörden. Diese verfügen über weitreichendere Kompetenzen (Einsichts- und Kontrollrechte, Verfügungsgewalt etc.) als der Eidgenössische Datenschutzbeauftragte (EDÖB) im Rahmen seiner Aufsicht über Privatpersonen. Zudem ist das kantonale Datenschutzrecht in mancher Hinsicht strenger ausgestaltet als die privatrechtlichen Bestimmungen des DSG. Beispielsweise müssen sich Datenbearbeitungen durch öffentliche Organe auf eine gesetzliche Grundlage stützen und zur Erfüllung der öffentlichen Aufgabe geeignet und erforderlich sein. Weitere Anforderungen betreffen etwa die Information der Betroffenen über die Datenbeschaffung, Meldepflichten gegenüber den Datenschutzbeauftragten und die Durchführung von Datenschutz-Folgenabschätzungen.

Der Begriff des öffentlichen Organs wird je nach Kanton unterschiedlich definiert. In der Regel werden darunter Personen und Organisationen verstanden, die i) öffentlich-rechtlich organisiert sind und/oder ii) öffentliche (d.h. kantonale oder kommunale) Aufgaben wahrnehmen. Die Frage, ob ein Spital oder Pflegeheim grundsätzlich dem DSG oder dem kantonalen Datenschutzrecht untersteht, hängt somit davon ab, ob es datenschutzrechtlich als Privater oder als öffentliches Organ gilt. Hierbei lassen sich folgende Kategorien bilden:

Private Institutionen ohne Leistungsauftrag

Am einfachsten ist die Rechtslage bei rein privaten Spitälern und Pflegeheimen, die keinen



kantonalen oder kommunalen Leistungsauftrag wahrnehmen beziehungsweise auf keiner Spital- oder Pflegeheimliste aufgeführt sind. Dies ist etwa der Fall bei reinen Vertragsspitälern oder privaten Alters- und Pflegeheimen ohne Listenplatz. Solche Institutionen unterstehen ausschliesslich den Vorschriften des DSG über die Datenbearbeitungen privater Personen und damit der (beschränkten) Aufsicht des EDÖB. Das kantonale Datenschutzrecht kommt nicht zur Anwendung.

Öffentlich-rechtliche Institutionen

Öffentlich-rechtlich organisierte Spitäler und Pflegeheime, seien es Verwaltungseinheiten (wie im Fall der Zürcher Stadtspitäler Triemli und Waid) oder eigenständige juristische Personen des öffentlichen Rechts (so das Universitätsspital Zürich als öffentlich-rechtliche Anstalt), gelten teilweise bereits wegen ihrer öffentlich-rechtlichen Organisationsform als öffentliche Organe im datenschutzrechtlichen Sinn. Teilweise bildet aber auch die Ausführung öffentlicher Aufgaben das relevante Anknüpfungskriterium für das kantonale Datenschutzrecht. Die Erfüllung von kantonalen oder kommunalen Leistungsaufträgen im Bereich der Spitalversorgung oder der Pflege stellt eine solche öffentliche Aufgabe dar. Entsprechend unterstehen öffentlich-rechtliche Spitäler und Pflegeheime zumindest im Bereich des Leistungsauftrags dem kantonalen Datenschutzrecht.

Privatrechtlich organisierte Institutionen mit Leistungsauftrag

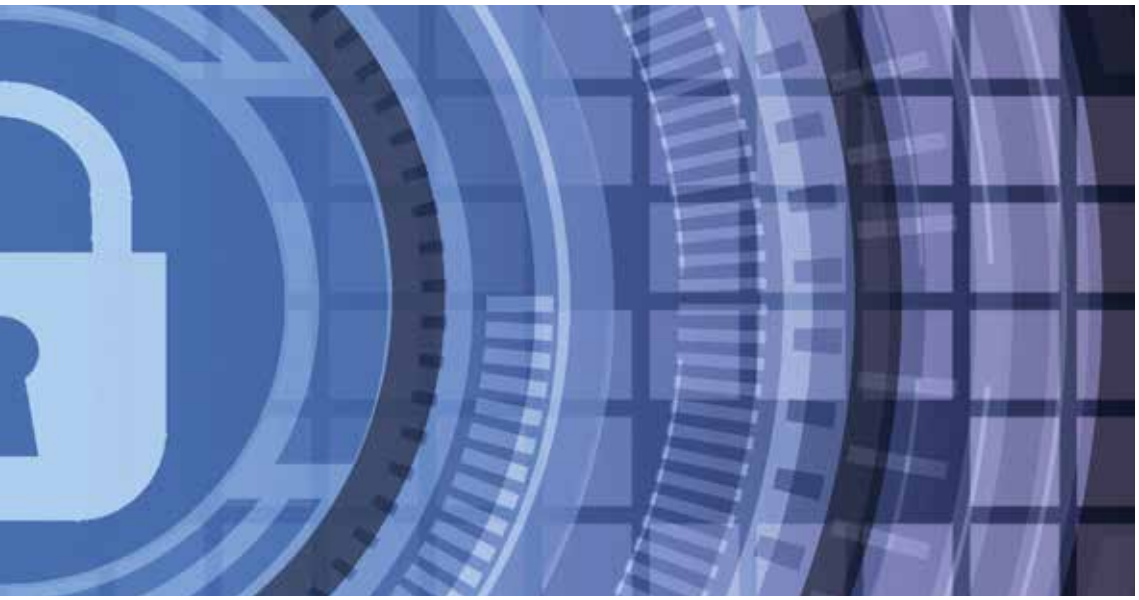
Privatrechtlich organisierte Spitäler und Pflegeheime unterstehen als Private zwar im Grundsatz dem DSG. Im Umfang ihres kantonalen Leistungsauftrags gelten sie allerdings, gleich wie öffentlich-rechtliche Institutionen, gleichwohl als kantonale öffentliche Organe und unterstehen insoweit dem kantonalen Datenschutzrecht. Allerdings gilt dies oftmals nur, soweit sie eine öffentliche Aufgabe erfüllen (so etwa das Zürcher Gesetz über die Information und den Datenschutz, ZH-IDG) bzw. soweit ihnen die Erfüllung öffentlicher Aufgaben von Kanton oder Gemeinden übertragen ist (so etwa das Informations- und Datenschutzgesetz Basel-Stadt, BS-IDG, und das Datenschutzgesetz des Kantons Bern, BE-KDSG). Die Einschränkung «soweit» legt den Schluss nahe, dass Organisationen zumindest in denjenigen Bereichen, in denen sie keine öffentliche Aufgaben (d. h. Leistungsaufträge) erfüllen, aus dem Anwendungsbereich des kantonalen Datenschutzrechts fallen. Hierzu gehören etwa der Gastronomie- und Hotelleriebereich von Pflegeheimen.

Ausnahmen für wettbewerbliche, privatrechtliche Tätigkeiten

In verschiedenen Kantonen, etwa in Zürich, Bern und Basel-Stadt, sehen die Datenschutzgesetze zusätzlich vor, dass öffentliche Organe vom Anwendungsbereich des IDG ausgenommen sind, die am wirtschaftlichen Wettbewerb teilnehmen und dabei «privatrechtlich» bzw. «nicht hoheitlich» auftreten. Die Tragweite dieser Ausnahmebestimmungen ist nicht abschliessend geklärt. Der Gesetzgeber hatte insbesondere (obschon nicht ausschliesslich) die Tätigkeiten von Kantonalbanken oder private Dienstleistungen von Elektrizitätswerken oder Gebäudeversicherern vor Augen. Diese Akteure sollten ihren privaten Konkurrenten datenschutzrechtlich ebenbürtig sein.

Nach einem restriktiven Verständnis kommen die genannten Bereichsausnahmen nur zum Tragen, wenn die betroffenen öffentlichen Organe am marktwirtschaftlichen Wettbewerb teilnehmen. Da im Bereich der stationären Spitalversorgung und der Pflegeversorgung zulasten der OKP nach bundesgerichtlicher Rechtsprechung kein Wettbewerb im privatwirtschaftlichen Sinn ▸▸

➡ Spitäler und Pflegeheime mit Leistungsaufträgen kommen grundsätzlich nicht darum herum, nach Massgabe des jeweils anwendbaren kantonalen Rechts zu eruieren, ob sie ausschliesslich dem (strengeren) öffentlichen Datenschutzrecht ihres Kantons oder zumindest bereichsweise den (liberaleren) privatrechtlichen Vorschriften des DSG unterstehen.



FOTOS: PIXABAY

herrscht (BGE 145 II 49 in Sachen GZO AG), profitieren die damit zusammenhängenden Datenbearbeitungen (wohl) nicht von der Bereichsausnahme. Diese Auffassung scheint etwa der Zürcher Regierungsrat in seinem Antrag zur Revision des Spitalplanungs- und -finanzierungsgesetzes zu vertreten.

Folgt man dieser am Wettbewerbsgedanken orientierten Auffassung, werden all diejenigen Datenbearbeitungen vom kantonalen Datenschutzrecht erfasst, die mit der Erfüllung des Leistungsauftrags fuktional zusammenhängen bzw. der Auftragserfüllung dienen. Dies dürfte insbesondere (aber nicht ausschliesslich) den Umgang mit den meisten medizinischen Patientendaten betreffen. Nur diejenigen Bereiche, in denen ein Spital oder Pflegeheim wie ein Privater am Markt auftritt, unterstehen den privatrechtlichen Bestimmungen des DSG. Dies gilt etwa für die Vertragsabwicklung bei der Mittelbeschaffung (z. B. die Verwaltung von Lieferantenangaben) oder für Dienstleistungen, die eine Institution losgelöst vom Leistungsauftrag für Dritte erbringt.



Sind diese Daten in einer Weise verschlüsselt, die es dem Cloud-Anbieter verunmöglichen, Rückschlüsse auf die Identität der Patienten zu ziehen, finden weder die kantonalen noch die bundesrechtlichen Datenschutzbestimmungen Anwendung.

Zu einem liberaleren Ergebnis gelangt man, wenn man die kantonalen Ausnahmeregelungen in Anlehnung an die Parallelbestimmung im DSG versteht. Nach dieser Bestimmung unterliegen Bundesorgane den Vorschriften für privatrechtliche Datenbearbeitungen, sobald sie privatrechtlich handeln. Nach der Rechtsprechung des Bundesverwaltungsgerichts zu Transportverträgen der SBB im öffentlichen Personalverkehr ist hierfür entscheidend, ob die betroffene Organisation hoheitliche Befugnisse in einem Über-Unterordnungsverhältnis ausübt, etwa indem sie Verfügungen erlässt. Das Handeln in privatrechtlichen Formen, insbesondere unter Verträgen, wird laut Gericht hiervon nicht erfasst. Die entsprechenden Datenbearbeitungen unterliegen daher den privatrechtlichen (nicht den öffentlich-rechtlichen) Vorschriften des DSG.

Überträgt man diese liberalere Auffassung auf die kantonale Ebene, fallen nur gerade diejenigen Bereiche unter das kantonale Datenschutzrecht, in denen Spitäler und Heime hoheitlich, d. h. insbesondere mittels Verfügung, handeln können. Dies ist etwa im Rahmen von öffentlichen Ausschreibungen oder im Personalwesen öffentlich-rechtlicher Institutionen der Fall. In allen übrigen Bereichen, namentlich auch was die medizinische Behandlung angeht, handeln sie zwar möglicherweise in den Formen des öffentlichen Rechts, jedoch regelmässig ohne Hoheitsgewalt. Entsprechend unterstehen die dazugehörigen Datenbearbeitungen den privatrechtlichen Bestimmungen des DSG. Diese Rechtsauffassung scheint sich bis anhin noch nicht durchgesetzt zu haben.

Praktische Bedeutung

Spitäler und Pflegeheime mit Leistungsaufträgen kommen grundsätzlich nicht darum herum, nach Massgabe des jeweils anwendbaren kantonalen Rechts zu eruieren, ob sie ausschliesslich dem (strengeren) öffentlichen Datenschutzrecht ihres Kantons oder zumindest bereichsweise den (liberaleren) privatrechtlichen Vorschriften des DSG unterstehen. Die Beantwortung dieser Frage hängt von der Auslegung der kantonalen Bestimmungen ab, wobei sich wie gezeigt oftmals verschiedene Auffassungen vertreten lassen.

Je nach kantonalem Recht sehen sich die meisten Institutionen mit Leistungsauftrag mit der Situation konfrontiert, dass sie für gewisse Datenbearbeitungen dem DSG und für andere dem kantonalen Datenschutzrecht unterstehen. Verzichtet eine Institution auf die einheitliche Anwendung des (strengeren) kantonalen Rechts auf sämtliche Datenbearbeitungen, setzt dies voraus, dass sich die betroffenen Datenbearbeitungen sinnvoll trennen lassen, nämlich in solche, die dem DSG unterstehen, und solche, die vom kantonalen Recht geregelt sind. Wo dies nicht möglich oder unpraktikabel ist, gelten aus verfassungsrechtlichen Gründen die strengeren Vorschriften des kantonalen Rechts. Dies ergibt sich auch aus dem Grundsatz «keine Flucht ins Privatrecht».

Rechtsfragen des Cloud-Computings

Wollen Spitäler Daten in die Cloud auslagern, stellt sich unter dem anwendbaren Rechtsrahmen die Frage nach der personenbezogenen Natur der zugänglich gemachten Daten. Sind diese Daten in einer Weise verschlüsselt, die es dem Cloud-Anbieter verunmöglichen, Rückschlüsse auf die Identität der Patienten zu ziehen (sog. relative Anonymität), finden weder die kantonalen noch die bundesrechtlichen Datenschutzbestimmungen Anwendung. Allerdings haben öffentliche Organe den Grundsatz zu beachten, dass sie auch über nicht personenbezogene Daten (Sachdaten) nicht völlig frei, sondern nur nach Massgabe des kantonalen Datenrechts (z. B. dem Transparenzprinzip) verfügen dürfen.

Massgebliche Regularien

Übermitteln Spitäler und Pflegeheime Cloud-Anbietern Personendaten, haben sie sowohl gemäss DSG wie kantonalem Recht neben den geheimnisschutzrechtlichen Bestimmungen (z. B. dem Berufs- und Amtsgeheimnis) die datenschutzrechtlichen Anforderungen an die Datensicherheit zu beachten. Insbesondere haben sie die angemessenen organisatorischen und technischen Massnahmen zu ergreifen. Um diese Anforderungen zu konkretisieren, haben kantonale Datenschutzbeauftragte Leitfäden herausgegeben.

Für den Kanton Zürich hat der Zürcher Datenschutzbeauftragte einen Leitfaden «Bearbeiten im Auftrag» veröffentlicht, der etwa die Anwendung der ISO 27002 und ISO 27001/BSI 200-1 vorsieht (s. Anhang 2, S. 12). Den Leitfaden «Bearbeiten im Auftrag» ergänzen im Kanton Zürich die Leitfäden «Verschlüsselung der Da-

ten im Rahmen der Auslagerung» und «Besondere datenschutzrechtliche Aspekte der Cloud-Nutzung». In technischer Hinsicht enthalten die Leitfäden vor allem Empfehlungen zur Verschlüsselung bzw. zum Schlüsselmanagement; in organisatorischer Hinsicht sehen sie vor allem Guidelines zur Vertragsgestaltung vor.

Risikoadäquate Massnahmen

Die Auslagerung und die ergriffenen Massnahmen sollten auf einer Risikoeinschätzung basieren, welche die Sensitivität der Daten, die mit der Auslagerung einhergehenden Risiken und das Auslagerungsinteresse des Spitals gewichtet und abwägt. Dabei sind die Grenzen im öffentlichen Recht enger gezogen als im Privatrecht: Während Privatpersonen Bearbeitungszwecke auch an marktwirtschaftlichen Erwägungen ausrichten können, dürfen öffentliche Organe Personendaten nur bearbeiten, soweit dies für die Erfüllung ihrer gesetzlichen Aufgaben erforderlich und im engeren Sinne verhältnismässig ist. Zudem werden sich öffentliche Organe stärker an den erwähnten Richtlinien der kantonalen Datenschutzbeauftragten orientieren müssen. Dies gilt auch für die Auslagerung von Datenbearbeitungen in die Cloud.

Für Spitäler und Pflegeheime empfiehlt sich, auch mit Blick auf die genannten Leitfäden, insbesondere,

- Patientendaten so weit wie möglich zu verschlüsseln, wobei das Schlüsselmanagement entweder bei der Auftraggeberin liegen oder durch vertragliche Absicherung sichergestellt sein sollte, dass der Auftragnehmer nur nach expliziter Einwilligung der Auftraggeberin oder nur soweit «unabdingbar» auf die Daten zugreift, und
- vertragliche Weisungs- und Kontrollrechte, Informations- und Geheimhaltungspflichten, Zugriffskonzepte sowie risikospezifische Sicherheitsanforderungen zu regeln.

Insbesondere wenn keine vollständige Datenverschlüsselung möglich ist, sind zusätzliche risikominimierende Massnahmen zu prüfen, darunter etwa:

- eine Auslagerung auf Server, die nur dem Spital bzw. Pflegeheim zugänglich sind («sichere Zone»),
- Vereinbarungen über Konventionalstrafen,
- eine Verpflichtung zur Einholung eines sog. Datenschutz-Revers der Mitarbeitenden des Cloud-Anbieters, d. h. eine Vereinbarung, die den Mitarbeitenden Verschwiegenheitspflichten eines öffentlichen Organs überbürdet;
- die Vereinbarung schweizerischen Rechts und eines schweizerischen Gerichtsstands.

Soweit Daten aus der klinischen Forschung ausgelagert werden, haben Spitäler zudem die Anforderungen des Humanforschungsrechts zu beachten. Für öffentlich-rechtlich organisierte Spitäler können weitere spezialgesetzliche Regelungen des kantonalen Rechts gelten (etwa das Zürcher Gesetz über die Auslagerung von Informatikdienstleistungen).

Auslagerungen ins Ausland

Nicht per se unzulässig ist eine Auslagerung ins Ausland, jedenfalls im Anwendungsbereich der Europäischen Datenschutzgrundverordnung. Ob sich die Infrastruktur und/oder der Sitz des Cloud-Providers bzw. dessen Unterauftragnehmer im Ausland befinden, ist nur einer von mehreren Faktoren, die es im Rahmen der Risikoeinschätzung zu gewichten gilt.

Allerdings sehen die kantonalen Leitfäden für Personendaten, die dem Berufsgeheimnis unterliegen, teilweise engere Grenzen für das Schlüsselmanagement vor, insbesondere wenn im Empfängerland – wie etwa in den USA – kein gleichwertiges gesetzliches Datenschutzniveau besteht. Danach muss der Schlüssel beim Auftraggeber verbleiben und darf dem Cloud-Anbieter nur im Sonderfall der Wartung und auf explizite Einwilligung des Spitals zugänglich sein. Sofern im Empfängerland kein ausreichendes Datenschutzniveau gewährleistet ist, müssen – das Fehlen anderer Rechtfertigungsgründe vorausgesetzt – zudem Standardvertragsklauseln vereinbart werden, die im Einzelfall risikoangemessene technische und organisatorische Massnahmen regeln.

DSG-Revision und Fazit

Im Verlauf des Jahres 2022 wird das revidierte DSG in Kraft treten, gefolgt von Reformen der kantonalen Datenschutzgesetze. An den in diesem Beitrag gezeigten Grundsätzen zur Frage des anwendbaren Rechts und den Regeln zur Cloud-Nutzung wird dies wenig ändern. Hinzu kommen jedoch verschärfte Informationspflichten bei Datenbearbeitungen durch Private, erweiterte Aufsichtsbefugnisse des EDÖB und gesteigerte Haftungsrisiken. Private wie öffentlich-rechtliche Einrichtungen werden darum besorgt sein, diesen Bestimmungen risikoangemessen Rechnung zu tragen.

Dazu müssen Spitäler und Pflegeheime in einem ersten Schritt prüfen, welches Datenschutzrecht auf die betreffende Bearbeitung zur Anwendung gelangt. Hierbei kommt es regelmässig darauf an, ob die Datenbearbeitung der Erfüllung einer öffentlichen Aufgabe dient und ob das insoweit anwendbare kantonale Recht seinerseits auf das DSG zurückverweist. Ist das anwendbare Recht bestimmt, haben Spitäler risikoadäquate vertragliche Vereinbarungen mit Cloud-Anbietern zu treffen, die angemessene technische und organisatorische Massnahmen vorsehen. Dazu zählen regelmässig ein Verschlüsselungsmanagement sowie Weisungs- und Kontrollbefugnisse, die eine rechtmässige Bearbeitung sicherstellen und Patientendaten in der Cloud vor unbefugtem Zugriff schützen.

Soweit Daten aus der klinischen Forschung ausgelagert werden, haben Spitäler zudem die Anforderungen des Humanforschungsrechts zu beachten.



Dr. iur. Martin Zobl, LL.M., ist Rechtsanwalt bei Walder Wyss. Zu seinen Schwerpunkten gehören die Beratung und Vertretung von Unternehmen im Gesundheitsrecht und im Bereich Life Sciences. Er publiziert und referiert regelmässig in seinen Fachgebieten.

› *Martin.zobl@walderwyss.com*



Dr. iur. Christine Schweikard, LL.M., Maître en droit, ist Rechtsanwältin bei Walder Wyss. Sie berät und vertritt im Schwerpunkt Klienten aus dem Gesundheitssektor in (lizenz- und forschungs-) vertrags-, verwaltungs- und datenschutzrechtlichen Fragen.