



ONLINEKOMMENTAR  
DER FREI ZUGÄNLICHE  
RECHTSKOMMENTAR

KOMMENTIERUNG ZU

# Art. 74 MepV

Eine Kommentierung von Philippe Fuchs / Erik Dinkel

Herausgegeben von Remus Muresan / Andrea Schütz

Stand der Bearbeitung: 18.02.2025

PDF erstellt am: 06.10.2026

DOI: 10.17176/20250218-194946-0

## ZITIERVORSCHLAG

Philippe Fuchs/Erik Dinkel, Kommentierung zu Art. 74 MepV, in: Remus Muresan/Andrea Schütz (Hrsg.), Onlinekommentar zur Medizinprodukteverordnung

Kurzzitat: OK-Fuchs/Dinkel, Art. 74 MepV N. XXX.

### **Art. 74 Cybersicherheit**

<sup>1</sup> Gesundheitseinrichtungen treffen alle technischen und organisatorischen Massnahmen, die nach dem Stand der Technik notwendig sind, um bei netzwerkfähigen Produkten den Schutz vor elektronischen Angriffen und Zugriffen sicherzustellen.

<sup>2</sup> Spitäler identifizieren, bewerten und dokumentieren die Massnahmen nach Absatz 1 gemäss den Grundsätzen eines Risikomanagementsystems. Dieses System ist integraler Bestandteil des Qualitätsmanagementsystems der Spitäler.

## GLIEDERUNG

|                                                                    |    |
|--------------------------------------------------------------------|----|
| I. Allgemeines.....                                                | 3  |
| II. Sorgfaltspflichten für Gesundheitseinrichtungen (Abs. 1) ..... | 4  |
| III. Risikomanagement für Spitäler (Abs. 2).....                   | 8  |
| IV. Rechtsfolgen bei Verletzung der Sorgfaltspflichten .....       | 9  |
| A. Zivilrechtliche Folgen .....                                    | 9  |
| B. Verwaltungsrechtliche Folgen .....                              | 10 |
| Literaturverzeichnis.....                                          | 11 |
| Materialienverzeichnis.....                                        | 11 |

## I. ALLGEMEINES

- 1 In den letzten Jahren hat sich gezeigt, dass Spitäler und andere Gesundheitseinrichtungen vermehrt zu beliebten Zielen von Cyberangriffen geworden sind.<sup>1</sup> Nicht nur in der Schweiz, sondern weltweit lässt sich diese Tendenz zu vermehrten Cyberangriffen auf Spitäler und Gesundheitseinrichtungen beobachten. Die Motivation dahinter ist klar: Ein Ausfall der technischen Infrastruktur (z.B. von lebenserhaltenden medizinischen Geräten oder des Klinikinformationssystems) in einem Spital kann katastrophale Folgen haben, weshalb solche Ziele für Cyberkriminelle besonders lukrativ erscheinen. Solche Cyberangriffe können für die betroffenen Gesundheitseinrichtungen einerseits verheerende finanzielle Folgen haben. Andererseits können sie negative Auswirkungen auf Patientinnen und Patienten haben, da lebenserhaltende medizinische Geräte betroffen sein können oder weil bereits geplante Operationen verschoben werden müssen.<sup>2</sup> Diese Problematik wurde erkannt und im Rahmen der Revision der Medizinprodukteverordnung im Jahr 2020 adressiert. Mit der Revision der Medizinprodukteverordnung, welche am 21. Mai 2021 in Kraft trat, wurde ein neuer Art. 74 MepV geschaffen, welcher Gesundheitseinrichtungen und Spitälern spezifische Sorgfaltspflichten in Zusammenhang mit Cybersicherheit auferlegt.
- 2 Abzugrenzen ist Art. 74 MepV dabei von den entsprechenden – bundesrechtlichen oder kantonalen – Datenschutzbestimmungen (z.B. Art. 8 DSG), welche dem Schutz von Personendaten dienen. Art. 74 MepV hingegen dient in erster Linie nicht dem Schutz von Patientendaten, sondern dem Schutz vor einem Ausfall der technischen Infrastruktur der Gesundheitseinrichtung durch elektronische Angriffe auf netzwerkfähige Medizinprodukte. Ganz voneinander trennen lassen sich die beiden Bereiche jedoch nicht, denn eine Verletzung von Art. 74 MepV kann auch eine Verletzung der datenschutzrechtlichen Sicherheitsbestimmungen (Art. 8 DSG) zur Folge haben, da zahlreiche netzwerkfähige Medizinprodukte (wie z.B. Computertomographen oder Ultraschall-Geräte) auch Patientendaten bearbeiten und sich diese Daten teilweise auf dem Medizinprodukt befinden.<sup>3</sup>
- 3 Darüber hinaus sind die Pflichten gemäss Art. 74 MepV von der Pflicht der Hersteller, sichere Medizinprodukte herzustellen und in Verkehr zu bringen, abzugrenzen. Gemäss Art. 6 Abs. 2 MepV müssen Medizinprodukte den grundlegenden Sicherheits- und Leistungsanforderungen nach Anhang I der Verordnung (EU) 2017/745 («EU-MDR») genügen. Anhang I der EU-MDR definiert in den Ziffern 17.2 sowie 17.4 allgemeine (Sicherheits-)Anforderungen in Zusammenhang mit Cybersicherheit für Produkte, zu deren Bestandteilen programmierbare Elektroniksysteme gehören, sowie Produkte in Form einer Software.<sup>4</sup> Bei Produkten, zu deren Bestandteilen Software gehört, oder bei Produkten in Form einer Software wird die Software entsprechend dem Stand der Technik entwickelt und hergestellt, wobei die Grundsätze des Software-Lebenszyklus, des Risikomanagements einschliesslich der Informationssicherheit zu berücksichtigen sind (Ziff. 17.2 von Anhang I der EU-MDR). Dabei haben die Hersteller Mindestanforderungen bezüglich Hardware, Eigenschaften von IT-Netzen und IT-Sicherheitsmassnahmen einschliesslich des Schutzes vor unbefugtem Zugriff festzulegen, die für den bestimmungsgemässen Einsatz der Software erforderlich sind (Ziff. 17.4 von Anhang I der EU-

1. Vgl. z.B. den Artikel in der NZZ vom 28.1.2020: «*Wir hatten ein Riesenglück*» – das Spital Wetzikon wurde vom derzeit aggressivsten Trojaner angegriffen».

2. Vgl. zum Thema Cybersicherheit in Spitälern auch Dinkel Erik, Cyber-Sicherheit in Spitälern, LSR 2 (2023), S. 59-60.

3. Grundsätzlich sollten diese mit dem Medizinprodukt erhobenen Patientendaten aus datenschutzrechtlicher Sicht ins Klinikinformationssystem der Gesundheitseinrichtung überführt und auf dem Medizinprodukt gelöscht werden. Die Praxis zeigt jedoch, dass dies nicht immer der Fall ist und Patientendaten teilweise für längere Zeit auf dem Medizinprodukt verbleiben, bevor sie gelöscht werden.

4. Vgl. zum Thema Cybersicherheit und Medizinprodukte Long William/Blythe Francesca/Sommer Josefine, Cybersecurity and Medical Devices, LSR 1 (2021), S. 58-62.

MDR). Diese Pflichten in Bezug auf Cybersicherheit – sozusagen als «First Line of Defense» gegen Cyberangriffe – treffen den Hersteller und müssen bereits bei der Entwicklung der Medizinprodukte berücksichtigt werden. Die Pflichten gemäss Art. 74 MepV treffen hingegen nicht den Hersteller, sondern die Anwender – also die Gesundheitseinrichtungen – und treten zu den Pflichten der Hersteller hinzu. Damit wird das Thema Cybersicherheit nicht nur auf Stufe Hersteller, sondern auch auf Stufe Anwender gesetzlich geregelt und es besteht ein doppelter Schutz in Bezug auf Cyberangriffe. In der Praxis zeigt sich jedoch, dass auf Stufe Hersteller die Cybersicherheitsbemühungen nicht immer den Erwartungen der Anwender entsprechen. Der Grund liegt unter anderem auch darin, dass solche netzwerkfähigen Medizinprodukte in aller Regel über eine umfangreiche Softwarekomponente verfügen, welche im Rahmen der Zertifizierung auf bestimmte Betriebssysteme abgestimmt (und zertifiziert) werden. Die Spitäler können jedoch ohne Mitwirkung der Hersteller keine Updates vornehmen und die Hersteller haben entsprechende Updates teilweise nicht verfügbar, da die Kompatibilität nach dem Update unter Umständen eine Re-Zertifizierung des Medizinprodukts erforderlich machen würde und dies von den Herstellern nicht gewünscht ist. Folglich sind Spitäler in der Praxis daher teilweise gezwungen, Medizinprodukte auf alter Software laufen zu lassen, welche unter Umständen als Einfallstor für Cyberangriffe dienen kann. Um dem entgegenzuwirken, sind in einem solchen Fall das Medizinprodukt und die Software vom restlichen System zu isolieren, damit ein Zugriff über dieses Medizinprodukt auf das restliche System des Spitals nicht mehr möglich ist.

## II. SORGFALTSPFLICHTEN FÜR GESUNDHEITSEINRICHTUNGEN (ABS. 1)

- 4 Abs. 1 von Art. 74 MepV verlangt von Gesundheitseinrichtungen, alle technischen und organisatorischen Massnahmen zu treffen, die nach dem Stand der Technik notwendig sind, um bei netzwerkfähigen Medizinprodukten den Schutz vor elektronischen Angriffen und Zugriffen sicherzustellen.
- 5 Diese Sorgfaltspflicht trifft gemäss Art. 74 Abs. 1 MepV Gesundheitseinrichtungen. Als **Gesundheitseinrichtung** gilt gemäss Art. 4 Abs. 1 lit. k MepV jede Organisation, deren Hauptzweck in der Versorgung oder Behandlung von Patientinnen und Patienten oder der Förderung der öffentlichen Gesundheit besteht. Dies entspricht der Definition in Art. 2 Ziff. 36 der EU-MDR und umfasst namentlich (privat- und öffentlich-rechtliche) Spitäler, aber auch Einrichtungen wie Laboratorien und andere (öffentliche) Gesundheitseinrichtungen, die zwar das Gesundheitssystem unterstützen, in denen Patienten aber nicht unmittelbar behandelt oder betreut werden.<sup>5</sup> Auch unter die Definition von Gesundheitseinrichtung fallen Arztpraxen und andere ambulante medizinische Einrichtungen, weshalb diese sich ebenfalls an die Sorgfaltspflichten gemäss Art. 74 Abs. 1 MepV halten müssen, sofern sie netzwerkfähige Medizinprodukte einsetzen. Nicht als Gesundheitseinrichtungen im Sinne von Art. 74 Abs. 1 MepV gelten hingegen Einrichtungen, die für sich in Anspruch nehmen, in erster Linie eine gesunde Lebensführung zu fördern, wie etwa Fitnessstudios, Heilbäder oder Wellnesszentren.<sup>6</sup>
- 6 Die Sorgfaltspflicht gemäss Abs. 1 greift nur bei **netzwerkfähigen Medizinprodukten**. Netzwerkfähig bedeutet, dass das Medizinprodukt in ein Netzwerk mit anderen Geräten eingebunden werden kann, so dass virtuell Informationen zwischen den verschiedenen netzwerkfähigen Produkten ausgetauscht und auf dieses von verschiedenen Standorten zugegriffen werden kann. Mit anderen Worten ist das Medizinprodukt nicht nur ins interne System der Gesundheitseinrichtung integriert, sondern auch von extern – via Fernzugriff – erreichbar. Der erläuternde Bericht des BAG spricht in

---

5. BAG, Erläuternder Bericht, S. 16.

6. BAG, Erläuternder Bericht, S. 16 f.

diesem Zusammenhang davon, dass Medizinprodukte direkt und dauerhaft mit dem Inter- und Intranet verbunden sind.<sup>7</sup> Ein externer Zugriff ist in vielen Fällen zwingend, damit der Hersteller entsprechenden (Fern-)Support erbringen kann. Es findet eine zunehmende Verschmelzung zwischen operationeller Technologie (also z.B. den Medizinprodukten) und der (restlichen) Informationstechnologie innerhalb der Gesundheitseinrichtung statt. Die Praxis zeigt, dass in der modernen Medizin zahlreiche Medizinprodukte netzwerkfähig sind – eine Medizin ohne digitale Vernetzung wird mehr und mehr undenkbar.<sup>8</sup> Beispiele von solchen netzwerkfähigen Medizinprodukten sind Computertomographen, mobile Röntgengeräte, Geräte zur Überwachung auf der Intensivstation (z.B. Patientenmonitoringsysteme), Beatmungs- und Anästhesiegeräte etc. Zu berücksichtigen ist ebenfalls, dass der Begriff des Medizinprodukts auch Software umfassen kann, sofern die Software die Voraussetzungen eines Medizinprodukts gemäss Art. 3 Abs. 1 MepV erfüllt – dies dürfte insbesondere auf Patientenmonitoringsoftware zutreffen.<sup>9</sup> Insofern bezieht sich die Sorgfaltspflicht gemäss Art. 74 Abs. 1 MepV auch auf Software.

- 7 Gemäss Art. 74 Abs. 1 MepV sind alle **technischen und organisatorischen Massnahmen** zu treffen, welche nach dem Stand der Technik notwendig sind, um den Schutz vor elektronischen Angriffen und Zugriffen sicherzustellen. Die MepV selbst enthält keine Definition der technischen und organisatorischen Massnahmen. Der Begriff der «technischen und organisatorischen Massnahmen» ist aber aus anderen Rechtsgebieten, insbesondere aus dem Datenschutzrecht, bekannt. So verlangt Art. 8 Abs. 1 DSGVO, dass Verantwortliche und Auftragsbearbeiter durch geeignete technische und organisatorische Massnahmen eine dem Risiko angemessene Datensicherheit gewährleisten müssen. In diesem Zusammenhang werden als technische Massnahmen jene Massnahmen beschrieben, die direkt mit einem Informationssystem oder mit Datenträgern zusammenhängen.<sup>10</sup> Als organisatorisch gelten hingegen Massnahmen, die das Umfeld des Systems, insbesondere die Personen, die es benutzen, sowie die Prozesse betreffen.<sup>11</sup> Das Nationale Zentrum für Cybersicherheit NCSC hat Empfehlungen zur Cybersicherheit im Gesundheitssektor erlassen.<sup>12</sup> Diese umfassen sowohl technische als auch organisatorische Massnahmen und werden vom NCSC (seit dem 1. Januar 2024 BACS<sup>13</sup>) als Mindestanforderungen angesehen. Zu beachten ist jedoch, dass diese Empfehlungen nicht spezifisch netzwerkfähige Medizinprodukte abdecken, sondern generell die gesamte Informationssicherheit einer Gesundheitseinrichtung umfassen.
- 8 Dieses Verständnis von technischen und organisatorischen Massnahmen aus anderen Rechtsgebieten lässt sich auf Art. 74 Abs. 1 MepV übertragen: Als **technische Massnahmen** gelten alle Massnahmen, die direkt mit dem Medizinprodukt, der IT-Infrastruktur der Gesundheitseinrichtung sowie der Schnittstelle zwischen Medizinprodukt und IT-Infrastruktur zusammenhängen. Beispiele von technischen Massnahmen sind: Verschlüsselung, Fire Walls, Back-ups, Passwortschutz, VPN bei Fernzugriff, Netzwerksegmentierung, automatische Desktop-Sperre etc. Dazu gehört auch das

---

7. BAG, Erläuternder Bericht, S. 48.

8. Dinkel Erik, Cyber-Sicherheit in Spitälern, LSR 2 (2023), S. 59; BAG, Erläuternder Bericht, S. 48.

9. Hingegen fallen Klinikinformationssysteme, welche lediglich der Speicherung, Archivierung und Kommunikation dienen, grundsätzlich nicht unter die Definition eines Medizinprodukts gemäss Art. 3 Abs. 1 MepV. Je nach Funktionen (insbesondere, wenn die Software eine medizinische Zweckbestimmung hat) kann aber auch ein Klinikinformationssystem ein Medizinprodukt darstellen. Vgl. zur Thematik Software und Medizinprodukt Fuchs Philippe, Software als Medizinprodukt LSR 3 (2018), S. 183 ff.

10. BSK DSGVO-Christa Stamm-Pfister, Art 8 N. 14; Baeriswyl Bruno, in: Baeriswyl/Pärli/Blonski (Hrsg), Stämpfli Handkommentar zum DSGVO, 2. Aufl., Art. 8 N. 33.

11. BSK DSGVO-Christa Stamm-Pfister, Art 8 N. 14; Baeriswyl Bruno, in: Baeriswyl/Pärli/Blonski (Hrsg), Stämpfli Handkommentar zum DSGVO, 2. Aufl., Art. 8 N. 34.

12. Empfehlungen zur Cybersicherheit im Gesundheitssektor vom 24.5.2022 des Nationalen Zentrums für Cybersicherheit NCSC.

13. Seit dem 1.1.2024 wurde aus dem NCSC das Bundesamt für Cybersicherheit (BACS).

Durchführen von periodischen bzw. vom Hersteller vorgeschriebenen (Software-)Sicherheitsupdates sowie die vom Hersteller vorgeschriebene bzw. regelmässige Wartung des Medizinprodukts. Das BACS nennt als technische Massnahmen insbesondere (a) die zeitnahe Überwachung der Endpunkte, (b) Offline-Backups bzw. Disaster Recovery, (c) Netzwerk-Segmentierung, (d) Schutz der Authentisierung (z.B. durch Multi-Faktor-Authentifizierung), (e) Blockierung von gefährlichen E-Mail Anhängen sowie (f) die Kontrolle der Ausführung von Dateien. Die technischen Massnahmen nach (b), (c) und (d) werden vom BACS als zwingend angesehen, diejenigen nach (a), (e) und (f) hingegen als freiwillig bzw. «kann»-Vorschriften.<sup>14</sup> Als **organisatorische Massnahmen** gemäss Art. 74 Abs. 1 MepV gelten hingegen jene Massnahmen, die das Umfeld des Medizinprodukts bzw. der IT-Infrastruktur betreffen, insbesondere die Personen, die das netzwerkfähige Medizinprodukt bzw. die damit zusammenhängende IT-Infrastruktur benutzen, sowie damit zusammenhängende Prozesse. Beispiele von organisatorischen Massnahmen sind Schulungen, Prozesse, Richtlinien, Reglemente, Verträge. Als organisatorische Massnahmen nennt das BACS unter anderem (a) das Patch- und Lifecycle-Management sowie (b) die zeitnahe Überwachung der Logdaten des Sicherheitsperimeters, wobei diese beiden Massnahmen vom BACS als zwingend angesehen werden.<sup>15</sup> Die Wichtigkeit von organisatorischen Massnahmen darf nicht unterschätzt werden, da die besten technischen Massnahmen (wie z.B. ein starker Passwortschutz) nur einen geringen Nutzen haben, wenn die bedienenden Personen diese Massnahmen wieder aushebeln (z.B. durch ein Post-it mit dem Passwort am netzwerkfähigen Medizinprodukt).<sup>16</sup> Folglich ist durch organisatorische Massnahmen (wie z.B. interne Reglemente, Mitarbeiterschulungen) sicherzustellen, dass die technischen Massnahmen ihre Wirkung entfalten können. Die Erfahrung der Autoren zeigt, dass sich in der medizinischen Praxis vor allem folgende organisatorische Massnahmen etabliert haben: Richtlinien, eLearnings, Schulungen und Trainings, interner Blog zum Thema Cybersicherheit etc. Jedoch haben sich in der Praxis auch das Führen eines Inventars der verwendeten netzwerkfähigen Medizinprodukte sowie standardisierte Sicherheitsbeurteilungen von neuen Gerätetypen, welche vor der Beschaffung durchgeführt werden, als Teil der organisatorischen Massnahmen durchgesetzt. Insbesondere grössere Spitäler werden aus Sicht der Autoren aufgrund von Art. 74 Abs. 1 MepV nicht darum herumkommen, klare Verantwortlichkeiten und dezidierte Funktionen mit ausreichend Ressourcen innerhalb der Organisation zu schaffen, welche sich dem Thema Cybersicherheit annehmen, damit den gesetzlichen Sorgfaltspflichten Rechnung getragen wird. Kleinere Gesundheitsinstitutionen müssen zumindest externen IT-Support haben, welcher auch das Thema Cybersicherheit im Pflichtenheft führt.

- 9 Die zu treffenden technischen und organisatorischen Massnahmen haben sich nach dem **Stand der Technik** zu richten. Auch dieser Begriff wird durch die MepV nicht näher definiert. «Stand der Technik» ist jedoch ein Begriff, dem im Rahmen der Entwicklung von Medizinprodukten ein hoher Stellenwert zukommt, ist doch in Bezug auf die grundlegenden Sicherheits- und Leistungsanforderungen gemäss Kapitel I von Anhang I EU-MDR der allgemein anerkannte Stand der Technik zugrunde zu legen. Jedoch enthält auch die EU-MDR keine allgemeine Definition, welche diesem Begriff mehr Konturen geben würde. Dem übrigen Schweizer Recht ist der Begriff des «Stand der Technik» geläufig: Gemäss Art. 3 Abs. 2 PrSG müssen Produkte in Bezug auf Sicherheit dem Stand des Wissens und der Technik entsprechen. Gemäss Art. 5 Abs. 1 lit. e PrHG haftet eine Herstellerin nicht, wenn sie beweist, dass der Produktfehler nach dem Stand der Wissenschaft und Technik im Zeitpunkt, in dem das Produkt in Verkehr gebracht wurde, nicht erkannt werden konnte. Aus Literatur und Rechtsprechung zu diesem Begriff im übrigen Schweizer Recht lässt sich folglich ableiten, dass

14. Empfehlungen zur Cybersicherheit im Gesundheitssektor, Fn 12, S. 1; zu den einzelnen technischen Massnahmen wird auf die Empfehlungen verwiesen.

15. Empfehlungen zur Cybersicherheit im Gesundheitssektor, Fn 12, S. 1; zu den einzelnen organisatorischen Massnahmen wird auf die Empfehlungen verwiesen.

16. Vgl. auch die Empfehlungen zur Cybersicherheit im Gesundheitssektor, Fn 12, S. 1.

der Stand der Technik nach objektiven Kriterien ermittelt werden und von der betreffenden wissenschaftlichen Gemeinschaft als seriös anerkannt sein muss.<sup>17</sup> In jedem Fall müssen für ein bestimmtes Medizinprodukt die spezifischen Anweisungen des Herstellers in Bezug auf Cybersicherheit (sowie allfällige Updates solcher Anweisungen) – falls es solche geben sollte – beachtet werden. Darüber hinaus empfiehlt es sich, die Empfehlungen des BACS zur Cybersicherheit im Gesundheitssektor zu beachten.<sup>18</sup> Diese Empfehlungen werden vom BACS als «best current practices» angesehen und können daher – zumindest aus Behördensicht – zur Konkretisierung der Sorgfaltspflichten von Art. 74 Abs. 1 MepV herangezogen werden, sofern sie sich auf netzwerkfähige Medizinprodukte beziehen. Es ist daher davon auszugehen, dass Behörden und Gerichte diese Empfehlungen des BACS im Einzelfall zur Beurteilung der technischen und organisatorischen Massnahmen bzw. der Einhaltung der Sorgfaltspflicht heranziehen werden, auch wenn sie für Gerichte nicht verbindlich sind. Was internationale (Selbstregulierungs-)Normen betrifft, so hat sich die ISO-Norm 27001 für Informationssicherheits-Managementsysteme als gängiger Standard etabliert. In der Praxis folgen viele Spitäler dieser Norm, auch wenn sie nicht offiziell ISO-zertifiziert sind.

- 10 Es ist zu empfehlen, diese Anforderungen, welche ein netzwerkfähiges Medizinprodukt insbesondere aus technischer Sicht erfüllen muss, bereits in den **Beschaffungsprozess** der Gesundheitseinrichtung einfließen zu lassen. Der Gesundheitseinrichtung sollte bereits zu Beginn der Beschaffung von netzwerkfähigen Medizinprodukten klar sein, welchen technischen und IT-sicherheitsrelevanten Standards das zu beschaffende Medizinprodukt genügen muss, damit eben auch die Cybersicherheit im Einzelfall gewährleistet ist. H+, der Verband der Schweizer Spitäler, hat dazu, in enger Zusammenarbeit mit den Verantwortlichen für die Cyber- und Informationssicherheit der Schweizer Spitäler, im Mai 2024 ein Merkblatt «IT-Grundsutzanforderungen an Systeme – Informationssicherheit und Datenschutz» herausgegeben, welches «*die minimalen technischen und organisatorischen Informationssicherheits- und Datenschutzanforderungen des Spitals an Systeme*», insbesondere an alle medizintechnischen Systeme, festlegt.<sup>19</sup> Dieses Merkblatt wurde unter Miteinbezug der aus Art. 74 Abs. 1 MepV fliessenden Sorgfaltspflichten erlassen, weshalb von Art. 74 Abs. 1 MepV betroffene Gesundheitseinrichtungen dieses Merkblatt als Hilfestellung beiziehen sollten, auch wenn es sich nicht um Spitäler handelt.<sup>20</sup> Ganz generell gilt jedoch, dass solchen Leitlinien und Merkblättern von Behörden (wie dem BACS) oder Verbänden (wie dem H+) keine Gesetzeskraft zukommt und daher weder für Gerichte noch für die Anwender rechtlich verbindlich sind.
- 11 Art. 74 Abs. 1 MepV stellt in Bezug auf den Stand der Technik – anders als z.B. Art. 5 Abs. 1 lit. e PrHG – nicht auf einen bestimmten Zeitpunkt ab. Folglich unterliegt das Verständnis des Begriffs «Stand der Technik» einem **zeitlichen Wandel**. Ändert sich der Stand der Technik in Bezug auf die Cybersicherheit und die angemessenen technischen und organisatorischen Massnahmen, welche für eine effektive Abwehr von Cyberangriffen implementiert werden sollten, hat die Gesundheitseinrichtung ihre getroffenen Massnahmen entsprechend anzupassen. Folglich muss die Gesundheitseinrichtung ihre technischen und organisatorischen Massnahmen zur Gewährleistung der Cybersicherheit regelmässig überprüfen, mit dem aktuellen Stand der Technik abgleichen und – falls notwendig – dem aktuellen Stand der Technik anpassen. Zumindest für Spitäler ergibt sich diese Pflicht zudem auch aus Abs. 2 von Art. 74 MepV, denn Teil eines effektiven Risikomanagementsystems ist auch die periodische Überprüfung des Risikos sowie die Angemessenheit der dagegen

17. BGE 137 III 226 E. 4.1; SHK PrHG Hess, 3. Auflage, N 65 ff. zu Art. 5; BSK OR I-Fellmann, Art. 5 PrHG N. 16 ff.

18. Vgl. Fn 12.

19. IT-Grundsutzanforderungen an Systeme, herausgegeben von H+ Die Spitäler der Schweiz, Ziff. 1.1 und 1.3; abrufbar unter [www.hplus.ch](http://www.hplus.ch).

20. So nimmt das Merkblatt in Ziff. 1.3 explizit Bezug auf Art. 74 MepV.

implementierten Massnahmen. In grundsätzlicher Hinsicht muss festgehalten werden, dass das Thema Cybersicherheit ein laufender Prozess und folglich nie abgeschlossen ist.

- 12 Gemäss dem Wortlaut von Art. 74 Abs. 1 MepV hat die Gesundheitseinrichtung **alle Massnahmen** zu treffen, die **notwendig sind**, um den **Schutz** vor elektronischen Angriffen und Zugriffen **sicherzustellen**. Art. 74 Abs. 1 MepV unterscheidet sich im Wortlaut insbesondere vom verwandten Art. 8 DSG, welcher eine «*dem Risiko angemessene Datensicherheit*» verlangt und damit im Bereich der Sicherheit für Personendaten das Verhältnismässigkeitsprinzip gesetzlich statuiert, weshalb z.B. auch Implementierungskosten bei der Beurteilung der Angemessenheit berücksichtigt werden dürfen.<sup>21</sup> Es stellt sich folglich die Frage, ob der Wortlaut «*alle Massnahmen, die notwendig sind, um den Schutz sicherzustellen*» in Art. 74 Abs. 1 MepV überhaupt Platz für das Verhältnismässigkeitsgebot, insbesondere das Element der Zumutbarkeit, lässt. Unseres Erachtens ist dies zu bejahen, denn eine absolute Sicherheit gegen Cyberangriffe existiert nicht, weshalb es daher stets nur um den angemessenen, nicht aber den absoluten Schutz gehen kann.<sup>22</sup> Aufgrund der betroffenen Rechtsgüter – die Gesundheit der Patienten – ist die Hürde für die Beurteilung der Angemessenheit jedoch höher anzusetzen als im Datenschutz. Folglich hat die Gesundheitseinrichtung unter Art. 74 Abs. 1 MepV nur, aber immerhin, verhältnismässige (also geeignete, erforderliche und auch zumutbare) Massnahmen zu implementieren, welche der Wichtigkeit der betroffenen Rechtsgüter Rechnung tragen.
- 13 Die technischen und organisatorischen Massnahmen müssen Schutz vor **elektronischen Angriffen und Zugriffen** gewährleisten. Mit anderen Worten geht es um den Schutz vor Cyberangriffen, also dem gezielten Angriff auf die IT-Infrastruktur und die verwendeten (netzwerkfähigen) Medizinprodukte von Gesundheitseinrichtungen durch Unberechtigte. Dabei muss unterschieden werden zwischen Angriffen, bei denen das Medizinprodukt selbst das eigentliche Angriffsziel ist und Angriffen, bei denen das Medizinprodukt als Einfallstor für Zugriffe auf die weitere IT-Infrastruktur der Gesundheitseinrichtung dient. Art. 74 Abs. 1 MepV deckt beide Arten von Angriffen ab und die technischen und organisatorischen Massnahmen müssen demnach auch beide Arten von Angriffen erfassen. Typische Cyberangriffe sind Malware, Phishing, Zero-Day-Exploits, DDoS-Angriffe oder Attacken, welche die Verfügbarkeit der Systeme beeinträchtigen (wie z.B. Ransomware). Nach Ansicht der Autoren sind grundsätzlich Ransomware-Attacken am gefährlichsten, da diese dazu führen, dass die Verfügbarkeit der Systeme nicht mehr gewährleistet ist, was aus operativer und medizinischer Sicht schwerwiegende Folgen sowohl für das Spital als auch die Patienten haben kann.

### III. RISIKOMANAGEMENT FÜR SPITÄLER (ABS. 2)

- 14 Anders als die Pflichten in Art. 74 Abs. 1 MepV, welche alle Gesundheitseinrichtungen treffen, die netzwerkfähige Medizinprodukte einsetzen, treffen die Pflichten gemäss Art. 74 Abs. 2 MepV nur die Spitäler.<sup>23</sup> Als Spitäler gelten gemäss Art. 4 Abs. 1 lit. 1 MepV Gesundheitseinrichtungen, in denen durch ärztliche und pflegerische Hilfeleistungen stationäre Behandlungen von Krankheiten oder stationäre Massnahmen der medizinischen Rehabilitation oder stationäre medizinische Massnahmen zum Zwecke der Ästhetik durchgeführt werden. Entscheidendes Abgrenzungskriterium zu Arztpraxis bzw. anderen (ambulanten) Gesundheitseinrichtungen ist die stationäre Behandlung von Patienten. Gemäss Art. 74 Abs. 2 MepV müssen solche Einrichtungen die technischen und organisatorischen Massnahmen gemäss den Grundsätzen eines Risikomanagementsystems identifizieren, bewerten und dokumentieren. Dabei muss dieses Risikomanagementsystem integraler Bestandteil des Qualitätsmanagementsystems des Spitals sein.

---

21. BSK DSG-Christa Stamm-Pfister, Art 8 N. 18.

22. Vgl. zur Datensicherheit BSK DSG-Christa Stamm-Pfister, Art 8 N. 20.

23. Was ein bewusster Entscheid des Gesetzgebers war, vgl. BAG, Erläuternder Bericht, S. 48.

- 15 Die Praxis zeigt, dass ein umfassendes Risikomanagement auch in Spitälern zum Standard gehört.<sup>24</sup> In Bezug auf die Grundsätze eines effektiven Risikomanagementsystems wird auf die entsprechende Literatur verwiesen.<sup>25</sup> Art. 74 Abs. 2 MepV verpflichtet Spitäler in Bezug auf das Risiko «Cybersicherheit» die gemäss Abs. 1 getroffenen technischen und organisatorischen Massnahmen als Teil des Risiko- und Qualitätsmanagements zu identifizieren, bewerten und dokumentieren, womit – zumindest in Bezug auf Cybersicherheit – eine gesetzlich statuierte Pflicht für Spitäler zum Risikomanagement eingeführt wird. In der Praxis dürfte die Bedeutung dieser Bestimmung jedoch gering sein, da das Risikomanagement für Spitäler bereits vor Inkrafttreten von Art. 74 Abs. 2 MepV eine entscheidende Rolle spielte und auch das Thema Cybersicherheit – als ein gewichtiges Risiko – abgedeckt hat.

## IV. RECHTSFOLGEN BEI VERLETZUNG DER SORGFALTSPFLICHTEN

### A. Zivilrechtliche Folgen

- 16 Im Falle der **Nichtbeachtung** der durch Art. 74 MepV statuierten **Sorgfaltspflichten** stellt sich die Frage nach den **rechtlichen Konsequenzen**. Insbesondere ist an Situationen zu denken, in denen ein Cyberangriff dazu führt, dass lebenserhaltende Medizinprodukte ausfallen und zum Tod oder einer schweren Schädigung von Patienten führen. Darüber hinaus sind auch zahlreiche andere Konstellationen denkbar, wie z.B. die Verschiebung von lebenswichtigen Operationen oder die Fehlfunktion von medizinischen Geräten. Zu unterscheiden ist dabei in grundsätzlicher Hinsicht, ob es sich um eine private oder eine öffentlich-rechtliche Gesundheitseinrichtung handelt. Diese Qualifikation entscheidet darüber, welches Haftungsrecht Anwendung findet. Vorliegend soll nicht weiter auf diese Unterscheidung eingegangen werden, sondern es wird diesbezüglich auf die einschlägige Literatur und Rechtsprechung verwiesen.<sup>26</sup>
- 17 Besteht ein (privatrechtliches) Vertragsverhältnis zwischen Spital und Patient, richtet sich eine allfällige Haftung des Spitals nach Art. 97 Abs. 1 OR: Kann die Erfüllung der Verbindlichkeit überhaupt nicht oder nicht gehörig bewirkt werden, so hat der Schuldner für den daraus entstehenden Schaden Ersatz zu leisten, sofern er nicht beweist, dass ihm keinerlei Verschulden zur Last falle.<sup>27</sup> Haftungsvoraussetzungen von Art. 97 Abs. 1 OR sind demnach (a) Verletzung einer vertraglichen Pflicht, (b) ein daraus entstandener Schaden, (c) adäquater Kausalzusammenhang zwischen Vertragsverletzung und dem entstandenen Schaden, sowie (d) ein Verschulden (wobei dieses im Rahmen von Art. 97 Abs. 1 OR vermutet wird). Im Rahmen der Verletzung einer vertraglichen Pflicht ist vorliegend insbesondere die nichtgehörige Erfüllung bzw. die Schlechterfüllung – also die positive Vertragsverletzung – von Interesse. Der Schuldner erbringt zwar eine Leistung, diese weist aber nicht die vertragsgemässe Qualität auf bzw. entspricht nicht der unter dem Vertrag geschuldeten Sorgfalt.<sup>28</sup> Dabei wird in grundsätzlicher Hinsicht zwischen den eigentlichen Haupt- und den Nebenpflichten unterschieden. Zu den Nebenpflichten gehören unter anderem Verhaltenspflichten, die zum Zweck haben, die Hauptleistung zu ergänzen und deren ordnungsgemässe Erfüllung zu sichern bzw. den Vertragszweck zu erreichen, namentlich Schutz-, Obhuts-, Beratungs-, Unterlassungs-, Informations-

24. In Bezug auf das Universitätsspital Zürich vgl. z.B. Pfaff, Dieter/Thomet, Ursula, Risikomanagement des Universitätsspitals Zürich, Expert Focus 12 (2017), S. 953-959.

25. Statt vieler: Bühr, Daniel Lucien, Good Governance von Aufsicht und Kontrolle im Unternehmen, SJZ 118 (2022), S. 7 ff.; Bielefeld Jörg, Kressin Bernhard, Zawilla Peter, Wirksame Organisations-, Risiko- und Compliance-Kultur zur Haftungsvermeidung, CB 2020, S. 205 ff.

26. Vgl. statt vieler Gächter Thomas/Rütsche Bernhard, Gesundheitsrecht, 4. Auflage, Basel 2018, N. 293 f.

27. Grundsätzlich kann sich ein Patient auch auf die ausservertragliche Haftung gemäss Art. 41 OR stützen, wobei eine vertragliche Haftung für den Patienten aufgrund der Vermutung des Verschuldens günstiger ist.

28. BSK OR I-Wiegand, Art. 97 N. 25 ff.

und Aufklärungspflichten.<sup>29</sup> Die Sorgfaltspflichten, welche aus Art. 74 MepV in Bezug auf die Cybersicherheit resultieren, lassen sich basierend auf dem vorstehend Ausgeführten als vertragliche Nebenpflichten qualifizieren, denn es handelt sich um Verhaltenspflichten, welche die ordnungsgemässe Erfüllung der Hauptleistung sichern sollen. Es handelt sich mithin um eine Schutzpflicht des Spitals gegenüber dem Patienten.

- 18 Wann liegt konkret eine Verletzung der aus Art. 74 Abs. 1 MepV resultierenden Sorgfaltspflicht vor? Wie vorgängig dargelegt, geht es um den angemessenen Schutz vor elektronischen Angriffen und Zugriffen. Dieser angemessene Schutz ist anhand eines objektiven Massstabs im Einzelfall zu bestimmen. Merkblätter und Leitlinien – wie diejenigen des BACS oder von H+ – können als Hilfestellung zur Konkretisierung dieses objektiven Massstabs hinzugezogen werden, jedoch vermag die Nichteinhaltung von in solchen Leitlinien oder Merkblättern enthaltenen Empfehlungen nicht automatisch eine Sorgfaltspflichtverletzung zu begründen. In der Praxis ist betroffenen Unternehmen jedoch zu empfehlen, sich an solchen Leitlinien und Merkblätter von Expertengruppen zu orientieren und ihre Sicherheitsvorkehrungen anhand dieser Empfehlungen auszugestalten.
- 19 Eine Verletzung der Sorgfaltspflichten von Art. 74 Abs. 1 MepV kann daher – sofern die übrigen Haftungsvoraussetzungen von Art. 97 OR erfüllt sind – zu einer Haftung der Gesundheitseinrichtung gegenüber den betroffenen Patienten führen, wobei die Haftungsvoraussetzungen durch den betroffenen Patienten nachgewiesen werden müssen (Art. 8 ZGB). In der Praxis dürfte insbesondere der Beweis der Sorgfaltspflichtverletzung aufgrund mangelnder Einsicht in die IT-Infrastruktur der Gesundheitseinrichtung nicht leicht gelingen. Der Umstand, dass ein Angriff bzw. Zugriff stattgefunden hat, reicht allein für den Beweis der Sorgfaltspflichtverletzung nicht aus. Vielmehr muss nachgewiesen werden, dass die Gesundheitseinrichtung nicht alle (zumutbaren) technischen und organisatorischen Massnahmen getroffen hat, um solche Angriffe bzw. Zugriffe zu verhindern. Insofern ist zu verlangen, dass die betroffene Gesundheitseinrichtung im Rahmen ihrer prozessualen Mitwirkungspflicht gemäss Art. 160 Abs. 1 ZPO die notwendige Dokumentation zur IT-Sicherheit herauszugeben hat.<sup>30</sup> Verweigert die Gesundheitseinrichtung unberechtigterweise die Mitwirkung und die Herausgabe der Dokumentation zur IT-Sicherheit, so hat dies das Gericht bei der Beweiswürdigung zu berücksichtigen (Art. 164 ZPO).

## B. Verwaltungsrechtliche Folgen

- 20 Neben den zivilrechtlichen sind auch die verwaltungsrechtlichen Folgen einer Verletzung von Art. 74 MepV zu beachten. Swissmedic als Vollzugsbehörde ist für die Marktüberwachung und den Vollzug der Medizinprodukteverordnung zuständig (Art. 66 Abs. 1 HMG). Die Kontrolle im Rahmen der Marktüberwachung umfasst unter anderem das Erfüllen der Pflichten der Wirtschaftsakteure (Art. 75 Abs. 1 MepV), folglich also auch die Umsetzung der aus Art. 74 MepV resultierenden Pflichten. Anlässlich der Swissmedic-Spitalinspektion 2023 in Bezug auf Medizinprodukte hat sich gezeigt, dass das Thema Cybersicherheit in 43% der Inspektionen von Abweichungen betroffen war.<sup>31</sup> Insbesondere zeigten sich in Spitälern Mängel im Bereich der dazugehörigen Prozesse und Schnittstellen sowie des Risikomanagements. Das Instrumentarium der zur Verfügung stehenden Verwaltungsmassnahmen zur Behebung solcher Mängel ist grundsätzlich nicht beschränkt, da Art. 66 Abs. 1 HMG vorsieht, dass alle Verwaltungsmassnahme getroffen werden können, die zum Vollzug des HMG erforderlich sind. In Art. 66 Abs. 2 HMG sind nicht abschliessend gewisse Massnahmen

---

29. BGer 4A\_307/2011 E. 3.1; BSK OR I-Wiegand, Art. 97 N. 34.

30. Vgl. dazu auch Lienhard Andreas, Beweislast und Beweislastumkehr, ZZZ 53 (2021), S. 402 f.

31. Swissmedic, Medizinprodukte Swissmedic-Spitalinspektionen 2023, 2024, S. 6.

enthalten, welche durch Swissmedic angeordnet werden können. In jedem Fall müssen die angeordneten Massnahmen dem Verhältnismässigkeitsprinzip genügen.

## LITERATURVERZEICHNIS

Baeriswyl Bruno, Kommentierung zu Art. 8, in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Stämpflis Handkommentar zum Datenschutzgesetz, 2. Aufl., Bern 2023.

Bielefeld Jörg, Kressin Bernhard, Zawilla Peter, Wirksame Organisations-, Risiko- und Compliance-Kultur zur Haftungsvermeidung, CB 2020, S. 205 ff.

Bühr Daniel Lucien, Good Governance von Aufsicht und Kontrolle im Unternehmen, SJZ 118 (2022), S. 7 ff.

Dinkel Erik, Cyber-Sicherheit in Spitälern, LSR 2/2023, S. 59 ff.

Fellmann Walter, Kommentierung zu Art. 5 PrHG, in: Widmer Lüchinger Corinne/Oser David (Hrsg.), Basler Kommentar, Obligationenrecht I, 7. Aufl., Basel 2020.

Fuchs Philippe, Software als Medizinprodukt LSR 3 (2018), S. 183 ff.

Lienhard Andreas, Beweislast und Beweislastumkehr, ZZZ 53 (2021), S. 389 ff.

Long William/Blythe Francesca/Sommer Josefine, Cybersecurity and Medical Devices, LSR 1 (2021), S. 58 ff.

Pfaff, Dieter/Thomet, Ursula, Risikomanagement des Universitätsspitals Zürich, Expert Focus 12 (2017), S. 953 ff.

Sidiropoulos Alexia, Haftung für Gerätefehler bei der medizinischen Diagnostik und Behandlung, Sicherheit & Recht 1 (2020), S. 49 ff.

Stamm-Pfister Christa, Kommentierung zu Art. 8, in: Vasella David/Blechta Gabor P. (Hrsg.), Basler Kommentar, Datenschutzgesetz Öffentlichkeitsgesetz, 4. Aufl., Basel 2024.

Wiegand Wolfgang, Kommentierung von Art. 97, in: Widmer Lüchinger Corinne/Oser David (Hrsg.), Basler Kommentar, Obligationenrecht I, 7. Aufl., Basel 2020.

## MATERIALIENVERZEICHNIS

Bundesamt für Gesundheit, Erläuternder Bericht zur Totalrevision der Medizinprodukteverordnung und Verordnung über klinische Versuche mit Medizinprodukten, Juli 2020 («BAG, Erläuternder Bericht»).