



Berlin, 20. Mai 2024

## Stellungnahme

der Gesellschaft für Informatik e.V. (GI)

# zum Referentenentwurf einer Verordnung zur Gesundheits-IT-Interoperabilitäts-Governance (GIGV-E)

Am 24. April 2024 hat das Bundesministerium für Gesundheit (BMG) den Referentenentwurf einer „**Verordnung zur Gesundheits-IT-Interoperabilitäts-Governance (GIGV-E)**“ veröffentlicht. Die **Fachgruppe Digital Health der Gesellschaft für Informatik (GI)** hat diesen Referentenentwurf mit großem Interesse zur Kenntnis genommen, da er wichtige **Fortschritte im Bereich der Standardisierung und Gemeinschaftsbeteiligung** im Gesundheitswesen anstrebt.

Grundsätzlich begrüßt die GI die Initiative des BMG, die Interoperabilität im Gesundheitswesen durch **klare Regelungen und Strukturen** zu verbessern. Insbesondere die vorgeschlagene Erweiterung der Aufgaben und des Kompetenzbereichs der bestehenden Koordinierungsstelle ist ein positiver Schritt, um mehr Verbindlichkeit hinsichtlich des Einsatzes der empfohlenen Standards zu schaffen. Weiterhin bietet die Einführung eines **einheitlichen Kommentierungs- und Stellungnahmeverfahrens** die Möglichkeit, den Feedbackprozess für eine breitere Gemeinschaft und nicht nur wenige Fachexpert\*innen zugänglich zu machen. Dies sehen wir als Schritt in die richtige Richtung, um praktikable Lösungen zu entwickeln und eine breite Akzeptanz der getroffenen Entscheidungen zu gewährleisten.

Gleichzeitig weisen wir darauf hin, dass weitere Maßnahmen erforderlich sind, um **Spezifität der Verordnung** zu steigern und die **Beauftragung von Softwarekomponenten** realistisch umzusetzen. So sollten insbesondere die Kapazitäten und Best-Practices der Industrie stärker berücksichtigt und die



organisatorische Interoperabilität mitbedacht werden. Hierfür bieten unsere folgenden Bemerkungen und Handlungsempfehlungen konkrete Ansatzpunkte, um die Interoperabilität im Gesundheitswesen nicht nur zu fordern, sondern auch praktisch umsetzbar zu gestalten.

Die erfolgreiche Implementierung und Wirksamkeit der Verordnung erfordern einerseits die präzise **Spezifizierung von Begrifflichkeiten** und die klare Definition von Verantwortlichkeiten. Nur so kann vermieden werden, dass Mehrdeutigkeiten zu Rechtsunsicherheiten und Inkonsistenzen in der Anwendung führen, welche die Compliance mit Interoperabilitätsvorgaben und deren Überwachung nachhaltig beeinträchtigen.

In diesem Zusammenhang weisen wir darauf hin, dass **§ 2 - Begriffsbestimmungen** der aktuellen Verordnung auf die Definition wichtiger Fachterminologien verzichtet. Um sicherzustellen, dass alle beteiligten Akteure ein klares und einheitliches Verständnis von Schlüsselbegriffen wie „Softwarekomponente“ und „Referenzarchitektur“ haben, sollten die bestehenden Begriffsdefinitionen der Verordnung dementsprechend erweitert werden.

Weiterhin ist auch die in **§ 3 - Expertengremium** festgehaltene, interdisziplinäre Zusammensetzung des Gremiums nicht ausreichend konkretisiert. Die GI schlägt deswegen vor, dass die sieben ernannten Mitglieder aus klar definierten Bereichen wie z. B. Forschung, Industrie, Verbände und Krankenkassen stammen sollten, um eine umfassende und repräsentative Vertretung der verschiedenen Interessen zu gewährleisten und so die Akzeptanz der Entscheidungen des Gremiums erhöhen.

Darüber hinaus ist der in **§ 6 Abs. 2 Satz 11** aufgeführte Verweis auf § 393 SGB V veraltet, da dieser Artikel am 26. März 2024 aufgehoben wurde. Da solche Ungenauigkeiten zu Verwirrung und rechtlichen Unsicherheiten führen können, sollten alle gesetzlichen Verweise innerhalb der Verordnung überprüft und gegebenenfalls an die geltende Rechtslage angepasst werden.

Obwohl Cybersicherheit ein kritischer Aspekt in der Gesundheits-IT ist, findet diese in **§ 6 - Wissensplattform für Interoperabilität und Cybersicherheit** kaum Berücksichtigung. Wir schlagen daher vor, den Begriff der Cybersicherheit aus dem Paragraphen zu entfernen, falls keine substantiellen Richtlinien vorgesehen sind.

Um die wirksame Umsetzung der Verordnung zu gewährleisten, ist es weiterhin zwingend notwendig, dass diese auch Maßnahmen zur **organisatorischen Interoperabilität** beinhaltet. So sollten Hersteller nicht nur zur Einhaltung von Interoperabilitätsstandards verpflichtet, sondern auch bei ihrer Umsetzung unterstützt werden. Hierbei müssen insbesondere notwendige



Unterstützungsstrukturen bereitgestellt werden, um Herausforderungen wie begrenzte Ressourcen, fehlendes Fachwissen und unzureichende Testinfrastrukturen zu bewältigen, welche die Compliance mit der Verordnung nachhaltig gefährden können.

In diesem Zusammenhang fordert die GI, dass **§ 17 - Geschäfts- und Verfahrensordnung des Kompetenzzentrums** auch Vorgaben für ein transparentes Releasemanagement der über die Wissensplattform angebotenen Artefakte beinhalten sollte. Dieses sollte es den Nutzer\*innen ermöglichen, Änderungen zwischen verschiedenen Versionen nachzuvollziehen (Changelog) und detaillierte Informationen und Empfehlungen zur semantisch und syntaktisch versionskompatiblen Transformation von Datenbeständen (Mappings) enthalten. Nur so kann die erfolgreiche Integration der Spezifikationen in die strategische Planung und den Arbeitsalltag der Hersteller gewährleistet werden. Weiterhin sollte § 17 auch klare Richtlinien und Leitfäden für die Veröffentlichung von Spezifikationen auf der Wissensplattform zur Verfügung stellen.

Gerade die in **§ 7 vorgesehene Beauftragung Dritter** erfordert sowohl bei der Erstellung und Veröffentlichung als auch bei der Wartung und Weiterentwicklung von Standards und Spezifikationen die Etablierung klarer Richtlinien, welche einheitliche Standards, Transparenz und Nutzerfreundlichkeit gewährleisten. Weiterhin kann durch die Festlegung detaillierter Vorlagen, Strukturen und Formatierungsrichtlinien sichergestellt werden, dass der Fokus auf der inhaltlichen Qualität der Artefakte liegt und nicht auf unnötigen visuellen oder technischen Verzerrungen.

Weiterhin weisen wir darauf hin, dass die in § 7 vorgesehene Beauftragung Dritter bei der Wartung und Weiterentwicklung von Softwarekomponenten mit signifikanten Risiken für die Informationssicherheit verbunden ist. So kann beispielsweise eine durch Dritte entwickelte Softwarekomponente, die auf einer Wissensplattform veröffentlicht wird, durch einen Zero-Day-Exploit (wie im Fall von Log4j) kompromittiert sein. Dies kann nicht nur in hohen Kosten und Systemausfällen sondern auch in einem erheblichen Vertrauensverlust der Nutzer\*innen resultieren. Die GI fordert deshalb, dass die Informationssicherheit einer Softwarekomponente je nach Spezifikationsart im Rahmen des **Thread Modeling** explizit betrachtet werden muss. Dies ist insbesondere dann wichtig, wenn eine bereitgestellte Softwarekomponente als Teil kritischer Infrastrukturen (KRITIS) zu betrachten ist. Hier müsste dann weiterführend geklärt werden, ob in solchen Fällen das Bundesamt für Sicherheit in der Informationstechnik (BSI) zuständig ist.



Zusätzlich werfen Szenarien, in denen eine **Softwarekomponente in medizinischen Produkten** verwendet wird, Fragen nach der Haftung bei ernsthaften Schadensfällen auf. Deshalb ist es von größter Wichtigkeit, dass Zweckbindung, Einsatzbereiche und Verantwortlichkeiten von Softwarekomponenten klar definiert sind und ein angemessenes Wartungsregime etabliert wird.

Hinsichtlich **§ 14 - Meldepflicht bei wesentlichen Änderungen an informationstechnischen Systemen** merken wir an, dass diese mit einer hohen Belastung für die Hersteller verbunden ist. So lässt sie sich in ihrer aktuellen Form nur schwer mit den vorherrschenden agilen, iterativ-inkrementellen und technisch automatisierten Arbeitsprozesse vereinbaren. Dies könnte die Akzeptanz zur Implementierung von Spezifikationen nachhaltig beeinträchtigen. Die GI schlägt daher eine Umkehrung des vorgesehenen Prozesses vor: Sollte ein Hersteller nicht den Anforderungen der Verordnung entsprechende Änderungen vornehmen und trotzdem Konformität anführen, ist dies mit harten Bußgeldern zu ahnden. Als Modell hierfür könnte das Medizinproduktegesetz (MPG) dienen, welches vorschreibt, Medizinprodukte vor der Etablierung und Inbetriebnahme auf dem europäischen Markt mit einer CE-Kennzeichnung zu versehen.

Hinsichtlich **§ 16 - Bericht über die Tätigkeiten des Kompetenzzentrums und des Expertengremiums** fordert die GI eine verstärkte Betonung des Berichts- und Evaluationsverfahrens. So sollte insbesondere §16 Abs. 1 Satz 2 erweitert werden und neben wesentlichen Kennzahlen zur Nutzung der Wissensplattform auch Informationen zur Akkreditierung, Zertifizierung und eingegangenen Beschwerden erfassen. Weiterhin sollten Umfrage- oder Evaluationsergebnisse hinsichtlich der Akzeptanz der Wissensplattform und der angebotenen Spezifikationen systematisch erhoben werden. Dies würde es ermöglichen, Trends frühzeitig zu erkennen und entsprechende Gegenmaßnahmen zu ergreifen und so die Wirksamkeit und Benutzerfreundlichkeit der Plattform kontinuierlich verbessern.

### **Über die Gesellschaft für Informatik e.V. (GI)**

Die Gesellschaft für Informatik e.V. (GI) ist die größte Fachgesellschaft für Informatik im deutschsprachigen Raum. Seit 1969 vertritt sie die Interessen der Informatikerinnen und Informatiker in Wissenschaft, Gesellschaft und Politik und setzt sich für eine gemeinwohlorientierte Digitalisierung ein. Mit 14 Fachbereichen, über 30 aktiven Regionalgruppen und unzähligen Fachgruppen ist die GI Plattform und Sprachrohr für alle Disziplinen in der Informatik. Weitere Informationen finden Sie unter [www.gi.de](http://www.gi.de).