GESELLSCHAFT
FÜR INFORMATIK

Berlin, 24. Januar 2025

Stellungnahme

der Gesellschaft für Informatik e.V. (GI)

zum Referentenentwurf zur C5-Äquivalenz-Verordnung

Stand: 19.12.2024

GESELLSCHAFT
FÜR INFORMATIK

Bisher gilt für den Austausch von Gesundheits- und Sozialdaten der durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickelte „Kriterienkatalog C5 (Cloud Computing Compliance Criteria Catalogue)“. Mit dem Referentenentwurf zur C5-Äquivalenz-Verordnung des Bundesministeriums für Gesundheit (BMG) soll den Herstellern und Anbietern von cloud-basierten informationstechnischen Systemen nun „eine stufenweise Migration“ der internen Sicherheitskontrollen auf den C5-Standard ermöglicht werden.

Die Gesellschaft für Informatik e.V. (GI) bezieht im Folgenden zum Referentenentwurf zur C5-Äquivalenz-Verordnung Stellung.

1) **Die Motivation zur Verordnung ist intransparent.**

Die GI kann die Notwendigkeit der Verordnung nicht bewerten, da ihr zur Verbreitung der vorgenommenen C5-Zertifizierungen im Gesundheitssektor keine Informationen vorliegen.[1] Die GI fragt daher das BMG, ob ihm Informationen zu einer unzureichenden Zahl von ausgestellten C5-Zertifikat vorliegen.

2) **Der hohe Schutzbedarf von Gesundheits- und Sozialdaten muss trotz allgemeiner Standards berücksichtigt werden.**

Die GI begrüßt die Bemühungen, einheitliche Standards für das Teilen von Gesundheits- und Sozialdaten über cloudbasierte Informationssysteme aufzustellen. Gesundheits- und Sozialdaten sind jedoch besonders sensibel. Standards für diese Daten sollten entsprechend hohen Anforderungen genügen. Die in der C5-Äquivalenz-Verordnung aufgeführte ISO 27001 bzw. der IT-Grundschutz des BSI sind nicht auf diese Art Daten ausgerichtet. Die GI weist daher darauf hin, dass die besonderen Risiken und Herausforderungen im Gesundheitssektor sowie der hohe Schutzbedarf bei der Verarbeitung sensibler Daten durch entsprechende Abwägungen und gegebenenfalls entsprechende Auslegungs-/Bewertungsmaßgaben berücksichtigt werden sollte.

[1] Das BSI informiert auf ihrer Webseite, dass es nicht möglich sei, eine garantiert vollständige Liste mit allen Anbietern und ihren Diensten zu führen, die ein C5-Testat besitzen. Grund sei, dass Cloud-Anbieter bisher selbst bestimmen können, ob sie über erfolgte C5-Prüfungen öffentlich berichten.

3) Das Ziel müssen spezifische und strengere Standards sein.

Ausgehend von der Annahme, dass zu wenig Unternehmen die C5-Äquivalenz-Zertifizierung durchlaufen haben, fasst die GI die vorliegende Äquivalenzverordnung als akzeptable Übergangslösung auf. Den Vorschlag, die ISO 27001 bzw. den IT-Grundschutz des BSI vorübergehend als Standard zu akzeptieren, ist ein gangbarer Ansatz, der bereits erfolgreich im Finanzsektor beschritten wurde.[2] In der C5-Äquivalenzverordnung fehlt jedoch ein klarer (zeitlicher und inhaltlicher) Maßnahmenplan, der den Weg hin zu spezifischeren, verpflichtenden Standards, die einem hohen Schutzbedarf gewährleisten, deutlich aufzeigt.

Das Ziel muss bleiben , spezifischere und strengere Standards zu etablieren. Diese müssen auf die Befriedigung des hohen Schutz- bzw. Sicherheitsbedarfs von Gesundheits- und Sozialdaten zugeschnitten sein. Der vorliegende Vorschlag ist eine Lösung für einen befristeten Einsatz. Diese Befristung sollte klar herausgestellt werden. Der Vorschlag darf keinesfalls als Endpunkt verstanden werden.

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.

[2] Die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) setzte mit den Mindestanforderungen an das Risikomanagement von Banken (MaRisk) im Jahr 2009 zunächst auf „gängige Standards“ wie die ISO 27001 oder den BSI-Grundschutz.