GESELLSCHAFT
FÜR INFORMATIK

Berlin, 19. September 2025

Stellungnahme

der Gesellschaft für Informatik e. V. (GI)

Zur Community Draft-Version des Cloud Computing Compliance Criteria Catalogue (C5:2025) des Bundesamts für Sicherheit in der Informationstechnik (BSI)

GESELLSCHAFT
FÜR INFORMATIK

Die Gesellschaft für Informatik e.V. nimmt Stellung zum Community Draft-Version des Cloud Computing Compliance Criteria Catalogue (C5:2025) des Bundesamts für Sicherheit in der Informationstechnik (BSI).

Grundsätzliche Einschätzung

„Um C5-Stakeholdern die aktive Mitgestaltung des C5:2025 zu ermöglichen, wurden darüber hinaus die praktischen Erfahrungen von Cloud-Anbietern, -Prüfern sowie -Beraterinnen und -Beratern im Rahmen von Feedback-Gesprächen erhoben und in neue Kriterien oder die Anpassung bestehender Kriterien überführt“, heißt es auf der Webseite des BSI[1].

Die GI möchte hier generell anmerken, dass Standards – und insbesondere Zertifizierungs- und Audit-Standards – nicht ausschließlich denjenigen überlassen werden sollten, die anschließend selbst prüfen und sich an die eigenen Vorgaben halten müssen.

Im Falle des „Community Draft of the Cloud Computing Compliance Criteria Catalogue (C5:2025)“ des BSI folgt daraus erstens die klare Forderung nach einer institutionellen Trennung von Vorgabe und Kontrolle. Diese Lehre hätten wir aus den internationalen Skandalen um große Wirtschaftsprüfungsgesellschaften längst ziehen müssen. Zweitens ist angesichts der wachsenden Zahl von Normen und Anforderungen im Bereich IT-Sicherheit, Resilienz, technischer Datenschutz und der Bewertung von KI-Systemen der Bedarf an objektiven, daten- und evidenzbasierten und wissenschaftlich abgesicherten Prüfkriterien größer denn je.

Solche Kriterien sollten nicht – wie bisher häufig – „on the job“ im Rahmen praktischer Prüfungen durch Prüfungsgesellschaften entstehen oder in engem Einvernehmen mit den Geprüften (z. B. Herstellern von IT- oder KI-Systemen) entwickelt werden. Sie müssen vielmehr auf einer nachvollziehbaren, unabhängigen und wissenschaftlichen Grundlage beruhen, die sowohl fachliche Kompetenz als auch wissenschaftliche Unabhängigkeit sicherstellt.

Gerade im Bereich KI-Audit finden sich in der Gesellschaft für Informatik e.V. bereits Beispiele für systematisch entwickelte, wissenschaftlich fundierte Kriterien, Methoden und Verfahren[2]. Diese können als Blaupause für künftige Forschungs- und Entwicklungsprojekte dienen. Die Notwendigkeit solcher wissenschaftlich fundierter Prüfkriterien und unabhängiger Evaluationen – etwa zur Wirksamkeit von Gesetzen im

[1] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/C5_2025/C5_2025_node.html

[2] u.a. https://testing-ai.gi.de; Gesellschaft für Informatik (2018). Technische und rechtliche Betrachtungen algorithmischer Entscheidungsverfahren. Studien und Gutachten im Auftrag des Sachverständigenrats für Verbraucherfragen. Berlin: Sachverständigenrat für Verbraucherfragen.
https://gi.de/fileadmin/GI/Allgemein/PDF/GI_Studie_Algorithmenregulierung.pdf

Bereich Resilienz und IT-Sicherheit – betont die Gesellschaft für Informatik regelmäßig in Stellungnahmen zu aktuellen Gesetzesvorhaben[3].

C5 als verpflichtender Standard für die Umsetzung und Prüfung

Der C5 ist kein verpflichtender Standard, sondern ein Zertifizierungsrahmen, den Anbieter „auf dem Markt" erwerben können. Er stellt damit keine verbindliche Mindestanforderung dar, wie wir sie etwa aus anderen Bereichen der Produktsicherheit kennen. Für elektrische Geräte gilt beispielsweise die CE-Kennzeichnung als zwingende Voraussetzung für das Vermarkten und Verkaufen in der EU. Diese garantiert, dass grundlegende Anforderungen an Sicherheit, Gesundheitsschutz und Umweltschutz eingehalten werden – und sie ist für alle Produkte verpflichtend, unabhängig vom Herstellerland.

Eine vergleichbare Herangehensweise wäre auch für Cloud-Dienste und IT-Produkte sinnvoll: Mindestanforderungen an IT-Sicherheit und Datenschutz sollten obligatorisch sein und nicht in Form von komplexen, seitenlangen Katalogen variabler Kriterien (Basic, Additional Sharpening, Additional Complementing, Supplementary) ausgestaltet werden. IT-Sicherheitsexperte Bruce Schneier hat dies in Bezug auf IoT-Geräte mehrfach gefordert: Es brauche verbindliche Mindeststandards, nicht nur freiwillige Audit-Rahmenwerke[4]. Die Einführung solcher verpflichtenden Mindestanforderungen beim Marktzugang in der EU und den USA hätte zudem eine globale Signalwirkung. Aufgrund von Skaleneffekten („economies of scale") wäre es für internationale Anbieter wirtschaftlich kaum attraktiv, unterschiedliche Produktversionen für verschiedene Märkte zu entwickeln. Vielmehr würden strengere Standards in EU und USA faktisch weltweit für ein höheres Sicherheits- und Datenschutzniveau sorgen – und damit nicht nur die Souveränität, sondern auch die Usability und Resilienz von Cloud-Lösungen stärken.

Klare Terminologie für Rechtssicherheit in der Anwendung

„Die Community Draft-Version des C5:2025 wird im XLSX- und PDF-Format in englischer Sprache bereitgestellt. Die finale Version des C5:2025 wird im YAML-, XLSX- und PDF-Format auf Deutsch und Englisch veröffentlicht. Somit wird sie erstmals in einem maschinenlesbaren Format zur Verfügung stehen."[5]

Positiv hervorzuheben ist, dass der C5 künftig in maschinenlesbaren Formaten verfügbar sein wird – bei der Länge des Dokuments ein wichtiger Fortschritt. Kritisch zu

[3] Zuletzt beispielsweise in der Stellungnahme zum Referentenentwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz kritischer Anlagen vom 29. August 2025 (https://gi.de/fileadmin/GI/Allgemein/PDF/2025-09-03-Stellungnahme_GI_KRITIS-DachG.pdf).
[4] https://www.washingtonpost.com/posteverything/wp/2016/11/03/your-wifi-connected-thermostat-can-take-down-the-whole-internet-we-need-new-regulations/
[5] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/C5_2025/C5_2025_node.html

bewerten ist jedoch, dass der Community Draft zunächst nur auf Englisch veröffentlicht wurde. Für ein Dokument, das in Deutschland rechtliche und praktische Anwendung finden soll, ist dies problematisch – insbesondere, da Begriffe wie „Datenschutz“ oder „personenbezogene Daten“ im Deutschen fest verankert sind. So wird im Draft einmal von *privacy*, ein anderes Mal von *data protection* gesprochen, ohne dass klar ist, wann explizit der Datenschutz gemeint ist.

Ein Beispiel findet sich in der Formulierung: „This approach allows for the identification of trends and areas for improvement within the program while respecting employees' privacy requirements.“ (HR-03, S. 50). An anderer Stelle heißt es: „Applicable legal and regulatory requirements may exist, for example, in the areas of data protection, intellectual property rights or copyright.“ (SSO-01, S. 128). Auch beim Begriff der personenbezogenen Daten fehlt es an Konsistenz: Mal ist von *personal data*, mal von *sensitive* oder *confidential data* die Rede. Diese Unschärfen sind nicht nur terminologisch, sondern auch inhaltlich problematisch, da sie die konkrete Rechtsanwendung erschweren.

Ein derart wichtiges Dokument darf nicht in einer Terminologie verfasst sein, die variiert und damit Rechtsunsicherheit erzeugt. Stattdessen ist eine einheitliche Nomenklatur erforderlich, die klarstellt, welche Daten personenbezogene Daten sind – oder diese umfassen.

Dies betrifft besonders zwei Bereiche: Kryptographie und Logging/Monitoring.

- In Kapitel 5.8 *Cryptography and Key Management (CRY)* heißt es: „Objective: Ensure appropriate and effective use of cryptography to protect the confidentiality, authenticity or integrity of information.“ Die DSGVO adressiert in Art. 32 wie auch in Art. 25 ausdrücklich technische und organisatorische Maßnahmen, einschließlich Verschlüsselung, bei der Verarbeitung personenbezogener Daten. Da der Draft selbst mehrfach auf die GDPR/DSGVO verweist, sollte bei Cloud-Diensten präzisiert werden, ob bzw. dass personenbezogene Daten als eigenständige Subgruppe der dort genannten *information* oder *sensitive data* gelten (vgl. CRY-05 *Encryption of Sensitive Data*).

- Im Bereich Logging/Monitoring findet sich die Formulierung: „Personal data is automatically removed from the log data before the cloud service provider processes it, as far as technically possible. The removal is done in a way that allows the cloud service provider to continue to use the log data for the purpose for which it was collected.“ (OPS-11.01AC, S. 75). Hier wäre es empfehlenswert, die aktuelle Rechtsprechung in Deutschland zur Verarbeitung personenbezogener Daten im Kontext von Systemen zur Angriffserkennung (SzA) zu berücksichtigen. Entscheidend ist die präzise Ausgestaltung der Verträge mit Cloud-Anbietern, um den Vorgaben der DSGVO Rechnung zu tragen.

„In der Praxis wurde arbeitsteilige Datenverarbeitung bislang häufig vorschnell als Auftragsverarbeitung eingeordnet – und entsprechende Verträge geschlossen. Diese pauschale Einordnung greift jedoch zu kurz und wird der komplexen Realität insbesondere im Bereich von Systemen zur Angriffserkennung (SzA) […] nicht gerecht.

Denn ob ein Auftragsverhältnis, eine gemeinsame oder eine eigenständige Verantwortlichkeit vorliegt, richtet sich nach der tatsächlichen Ausgestaltung der Datenverarbeitung.“ (Filusch, K., Fünfstück, F. und Sowa, A. 2025. "Meine Daten – Deine Daten: Verantwortung und Verantwortungsübertragung für personenbezogene Daten aus Systemen zur Angriffserkennung“. In: DuD - Datenschutz und Datensicherheit 7/2025, Vol. 49, S. 474-480. S. 480).

Fazit

Der Community Draft des C5:2025 enthält positive Ansätze wie die maschinenlesbare Bereitstellung. Die terminologischen und konzeptionellen Unschärfen, insbesondere im Bereich Datenschutz und personenbezogener Daten, könnten jedoch die Praxistauglichkeit gefährden. Notwendig ist eine klare, einheitliche Terminologie, die sich eng an den etablierten Rechtsbegriffen der DSGVO orientiert und die besonderen Anforderungen an personenbezogene Daten im Kontext der Cloud eindeutig adressiert. Um es mit den Worten des Computer-Pioniers Edsger Dijkstra auszudrücken: „Simplicity is prerequisite for reliability“ – Einfachheit ist Voraussetzung für die Zuverlässigkeit (sinngemäß).

Kontakt

Nina Locher
Senior Referentin Cybersicherheitspolitik
Gesellschaft für Informatik e.V. (GI)

Geschäftsstelle Berlin
Weydingerstraße 14-16
10178 Berlin

E-Mail: nina.locher@gi.de

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.