Open Source Business Alliance

Bundesverband für digitale Souveränität e.V.

Referentenentwurf für ein Durchführungsgesetz zur Cyberresilienz-Verordnung

Stellungnahme der Open Source Business Alliance

2. April 2026

Die **Open Source Business Alliance (OSBA) – Bundesverband für digitale Souveränität e.V.** ist der Verband der Open-Source-Industrie in Deutschland und vertritt über **260 Mitgliedsunternehmen**. Die OSBA setzt sich als größter Open-Source-Verband Europas dafür ein, die zentrale Bedeutung von Open Source Software und offenen Standards für einen erfolgreichen digitalen Wandel im öffentlichen Bewusstsein nachhaltig zu verankern.

Kontakt:

Open Source Business Alliance – Bundesverband für digitale Souveränität e.V.
Pariser Platz 6a
10117 Berlin

Miriam Seyffarth
Leiterin Politische Kommunikation
Tel.: +49 (0) 30 20 65 39 221
E-Mail: seyffarth@osb-alliance.com
Internet: www.osb-alliance.com

Einleitung

Vor dem Hintergrund geopolitischer Entwicklungen rückt die Stärkung der digitalen Souveränität sowohl in der Industrie als auch in der Verwaltung immer mehr in den Fokus. Der Einsatz von Open Source Software ermöglicht aufgrund der Transparenz des Quellcodes Kontroll- und Gestaltungsfähigkeit über die eigene Software sowie Herstellerunabhängigkeit und ist damit eine entscheidende Grundvoraussetzung für die Erlangung digitaler Souveränität im Sinne des IT-Planungsrates.

Bereits heute enthalten ca. 96 Prozent aller Softwareprodukte Open-Source-Komponenten. Damit spielt Open Source Software eine entscheidende Rolle in der IT-Industrie und in der Gesamtwirtschaft – ohne Open Source läuft nichts. Somit ist auch die IT-Sicherheit von Open-Source-Lösungen zentral für die Funktionsfähigkeit von Wirtschaft und Verwaltung.

Als Open Source Business Alliance (OSBA) befürworten wir daher ausdrücklich das Ziel des Cyber Resilience Act (CRA) – zu deutsch: „Cyberresilienz-Verordnung“, die Qualität und Sicherheitsstandards von IT-Produkten zu erhöhen. Die Mitgliedsunternehmen unseres Verbands sehen sich in der Verantwortung, sichere und leistungsfähige Open-Source-Lösungen anzubieten und zu vertreiben.

Wir haben uns seit 2023 dafür eingesetzt, dass die Besonderheiten des Open-Source-Ökosystems im Cyber Resilience Act berücksichtigt werden, und haben hierfür im Rahmen von Stellungnahmen und Gastbeiträgen konkrete Vorschläge eingebracht.

Denn das Open-Source-Ökosystem ist u.a. durch komplexe Verflechtungen von ehrenamtlichen und kommerziellen Akteuren und Organisationen geprägt. Zudem unterscheiden sich die Entwicklungs- und Vertriebsmodelle von Open Source Software durch den offenen und kooperativen Ansatz sowie durch die Freiheiten, welche die Softwarelizenzen gewähren, zum Teil erheblich von den Entwicklungs- und Vertriebsmodellen proprietärer Software. Diesem Umstand wurde im CRA letztlich u.a. mit der neuen Rolle des „Open Source Software Steward“ Rechnung getragen.

Das Durchführungsgesetz zur Cyberresilienz-Verordnung muss deshalb ebenso wie auch der Cyber Resilience Act selbst die Besonderheiten des Open-Source-Ökosystems berücksichtigen, damit das bestmögliche Sicherheitsniveau von Open Source Software erreicht werden kann.

Im Folgenden machen wir daher einige konkrete Änderungsvorschläge für den vorliegenden Referentenentwurf.

1. Unterstützung der betroffenen Wirtschaftsakteure

Dem Referentenentwurf zufolge soll in § 67 des BSI-Gesetzes eine Unterstützung der betroffenen Wirtschaftsakteure bei der Erfüllung der CRA-Anforderungen durch das BSI eingefügt werden.

Wir fordern eine **Ergänzung** des entsprechenden Abschnittes:

> „Das Bundesamt unterstützt die betroffenen Wirtschaftsakteure, insbesondere kleine und mittlere Unternehmen ***und Hersteller von freien und quelloffenen Softwareprodukten sowie Verwalter von freier und quelloffener Software*** bei der Erfüllung der Anforderungen der Verordnung (EU) 2024/2847."

Neben kleinen und mittleren Unternehmen stehen auch Hersteller von Open-Source-Lösungen sowie die Verwalter von freier und quelloffener Software – die sogenannten „Open Source Software Stewards" – vor besonderen Herausforderungen bei der Umsetzung des CRA.

Open Source Software Stewards („Verwalter von freier und quelloffener Software„) sind zumeist Stiftungen oder Vereine, die ohne Gewinnerzielungsabsicht zentrale Open-Source-Komponenten weiterentwickeln und pflegen, die von kommerziellen Unternehmen verwendet und in ihre Produkte eingebaut werden. In dieser Funktion spielen sie eine zentrale Rolle für die Sicherheit der Open-Source-Lieferkette und sind gewissermaßen das Bindeglied zwischen den nicht-kommerziellen und den kommerziellen Akteuren im Open-Source-Ökosystem.

Die Anforderungen für Open Source Software Stewards sind weniger streng als für kommerzielle Akteure (Software-Hersteller), doch auch die Stewards müssen nach Artikel 24 CRA u.a. eine Cybersicherheitsstrategie entwickeln und dokumentieren sowie bestimmte Prozesse für den Umgang mit Sicherheitsvorfällen und Schwachstellen einrichten.

Die Organisationen, die künftig als „Open Source Software Stewards" fungieren, verfügen oftmals über sehr begrenzte personelle und finanzielle Mittel. Gerade mit Blick auf die gänzlich neuen Anforderungen, die sie jetzt erfüllen müssen, ihre mangelnde Erfahrung mit derartigen Auflagen, und ihre begrenzten Ressourcen ist eine Unterstützung durch offizielle Stellen wie das BSI unbedingt erforderlich.

Hersteller von Open-Source-Produkten („Hersteller von freien und quelloffenen Softwareprodukten") müssen im Großen und Ganzen die gleichen Anforderungen erfüllen wie die Hersteller proprietärer Software-Lösungen. Allerdings müssen die Hersteller von Open-Source-Produkten diese Anforderungen zum Teil anders umsetzen und priorisieren und es gibt auch einige Sonderregelungen. Das liegt

unter anderem daran, dass die Open-Source-Hersteller ihre integrierten Komponenten offen legen.

Open-Source-Hersteller sind konkret u.a. nach Art. 32 Abs. 5 CRA anders betroffen: Bei wichtigen Open-Source-Softwareprodukten wie z.B. einem Passwort-Manager kann die CRA-Konformität auch ohne Zertifizierung nur durch eigene Konformitätsbewertung erklärt werden, sofern die in Art. 31 CRA genannte technische Dokumentation zum Zeitpunkt des Inverkehrbringens dieser Produkte der Öffentlichkeit zugänglich gemacht wird.

Vor diesem Hintergrund muss das BSI Unterstützung für Open-Source-Hersteller u.a. bei der Erstellung von technischen Dokumentationen anbieten, die planmäßig veröffentlicht werden sollen.

2. Aufschiebende Wirkung bei Widerspruch und Klage gegen die Entscheidung der Marktüberwachungsbehöre

Im neuen § 65 des BSI-Gesetzes geht es um die Aufgaben des BSI als für den CRA zuständige Marktüberwachungsbehörde.

In § 65 Abs. 4 BSIG-E heißt es laut Referentenentwurf:

> „Widerspruch und Klage gegen die Entscheidung der Marktüberwachungsbehörde nach Absatz 1 haben keine aufschiebende Wirkung."

Wir fordern eine **ersatzlose Streichung** dieses Absatzes.

Diese Vorgabe belastet die betroffenen Wirtschaftsakteure in nicht erforderlicher Weise. Wenn es in einem konkreten Verfahren berechtigterweise keine aufschiebende Wirkung geben soll, reicht die Möglichkeit der regulären Anordnung nach § 80 Abs. 2 Nr. 4 Verwaltungsgerichtsordnung (VwGO).

Wenn das BSI beispielsweise bei einem „Verwalter von freier und quelloffener Software" (Open Source Software Steward) entscheidet, dass dieser doch ein Software-Hersteller im Sinne des CRA ist, hat ein Rechtsmittel gegen diese Entscheidung grundsätzlich aufschiebende Wirkung und die volle Rechtskraft (z.B. die Pflicht zur CE-Kennzeichnung) greift erst mit der Entscheidung über das Rechtsmittel. Besteht ein konkretes signifikantes Cybersicherheitsrisiko, dass eine unmittelbare Wirkung der Entscheidung rechtfertigt, so kann das BSI das Entfallen der aufschiebenden Wirkung mit entsprechender Begründung nach § 80 Abs. 2 Nr. 4 VwGO anordnen:

> „Widerspruch und Anfechtungsklage haben aufschiebende Wirkung. [...] Die aufschiebende Wirkung entfällt nur [...] in den Fällen, in denen die sofortige Vollziehung im öffentlichen Interesse oder im überwiegenden Interesse eines Beteiligten von der Behörde, die den Verwaltungsakt erlassen oder über den Widerspruch zu entscheiden hat, besonders angeordnet wird.

In seiner aktuellen Form würde § 65 Abs. 4 BSIG-E bedeuten, dass die Entscheidung des BSI sofortige Rechtskraft hätte und der betroffene Wirtschaftsakteur die aufschiebende Wirkung neben der Hauptentscheidung prozessual durchsetzen müsste.

3. Nutzung digital souveräner Lösungen bei der Umsetzung des CRA

Dem Referentenentwurf zufolge soll das BSI nach § 65 Abs. (3) BSIG-E eine Beschwerdestelle einrichten, bei welcher „Verbraucher Beschwerden einreichen können, die auf eine Nichteinhaltung der Verordnung (EU) 2024/2847 hindeuten."

Wir fordern, dass das BSI für diese neue **Beschwerdestelle** sowie für vergleichbare (ggf. neue) Portale und Lösungen im Rahmen der Umsetzung seiner Aufgaben, die im BSI-Gesetz im Zusammenhang mit dem CRA fest geschrieben werden, **digital souveräne Open-Source-Lösungen** einsetzt.

Das BSI darf bei der neuen Verbraucher-Beschwerdestelle nicht den gleichen Fehler machen wie bei dem kürzlich gestarteten NIS-2-Meldeportal.

Das neue BSI-Meldeportal, auf dem sich im Rahmen der NIS-2-Umsetzung knapp 30.000 Unternehmen und Behörden in Deutschland verpflichtend registrieren müssen, basiert auf einer Cloud-Infrastruktur von Amazon Web Services (AWS). An dieser Entscheidung gab es breite Kritik, der wir uns anschließen: Das Portal soll sensible Daten der kritischsten Unternehmen in Deutschland entgegen nehmen, dabei kann es laut Datenschutzerklärung des Portals „zu einer Übermittlung der IP-Adresse in die USA kommen".

Hierbei besteht u.a. die Gefahr, dass Unternehmen oder Bürger:innen davon absehen, das Meldeportal oder die CRA-Beschwerdestelle des BSI zu nutzen, da sie nicht sicher sein können, ob ihre sensiblen Daten sicher sind oder von unbefugten Dritten ausgelesen werden können.

Die Nutzung einer proprietären Cloud-Software, die nicht transparent kontrolliert oder unabhängig überprüft werden kann, und die zudem der US-amerikanischen Jurisdiktion des CLOUD Act und dem Zugriff der US-amerikanischen Regierung

unterliegt, **widerspricht in jeder Hinsicht den Zielen der Bundesregierung aus dem** Koalitionsvertrag**.** Dort heißt es schließlich:

> „Digitalpolitik ist Machtpolitik. Wir wollen ein digital souveränes Deutschland. Dazu werden wir digitale Abhängigkeiten abbauen [...] Wir definieren Ebenen übergreifend offene Schnittstellen, offene Standards und treiben Open Source mit den privaten und öffentlichen Akteuren im europäischen Ökosystem gezielt voran [...]. Dafür richten wir unser IT-Budget strategisch aus und definieren ambitionierte Ziele für Open Source."

Vor diesem Hintergrund muss das BSI bei der Einrichtung und Nutzung von Meldeportalen (NIS-2), Beschwerdestellen (CRA) oder vergleichbaren Plattformen auf digital souveräne Open-Source-Lösungen zurückgreifen, statt sensible Daten von deutschen Unternehmen oder Verbraucher:innen in die Hände außereuropäischer Hyperscaler zu legen. Immerhin hat sich das BSI im Rahmen seiner „Doppelstrategie zur digitalen Souveränität" auch das Ziel gesetzt, den „EU-Markt und die eigene Digitalindustrie" zu stärken.

Entsprechende Alternativen sind u.a. mit dem **Sovereign Cloud Stack**, der von unterschiedlichsten Anbietern in Deutschland betrieben werden kann und im kürzlich beschlossenen Deutschland-Stack explizit als zu nutzender Standard erwähnt wird, bereits verfügbar.

Fazit

Der Cyber Resilience Act erkennt Open Source Software als sicherheitsrelevanten Bestandteil digitaler Infrastruktur an und geht differenziert auf die besonderen Anforderungen und Konstellationen der Open-Source-Branche ein.

Daher muss auch das Durchführungsgesetz zur Cyberresilienz-Verordnung die Besonderheiten des Open-Source-Ökosystems aufgreifen und berücksichtigen und damit der Intention des CRA entsprechen.

Unsere Verbandsmitglieder befassen sich seit 2024 in einer eigenen Arbeitsgruppe intensiv mit dem CRA, seinen Anforderungen für unterschiedliche Software-Anbieter und Akteure, mit der Standardisierung in europäischen Standardisierungsgremien sowie mit der entsprechenden Technischen Richtlinie TR-03183 des BSI zur Umsetzung des CRA.

Wir stehen daher jederzeit mit unserer Expertise zu digitaler Souveränität, Open Source Software und dem Cyber Resilience Act für Rückfragen und Beratungen zur Verfügung.