

Stellungnahme des EDSA nach Artikel 64 DSGVO



Stellungnahme 34/2023 zu dem Entwurf eines Beschlusses der Aufsichtsbehörde Hessens (Deutschland) zu den verbindlichen internen Datenschutzvorschriften für Auftragsverarbeiter der Cerner-Gruppe

Angenommen am 13. Dezember 2023

Translations proofread by EDPB Members

Inhaltsverzeichnis

1	ZUSAMMENFASSUNG DES SACHVERHALTS.....	5
2	BEWERTUNG.....	5
3	SCHLUSSFOLGERUNGEN.....	6
4	ABSCHLIEBENDE BEMERKUNGEN.....	6

Der Europäische Datenschutzausschuss —

gestützt auf Artikel 63, Artikel 64 Absatz 1 Buchstabe f und Artikel 47 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (im Folgenden „**DSGVO**“),

gestützt auf das Abkommen über den Europäischen Wirtschaftsraum (im Folgenden „**EWR**“), insbesondere auf Anhang XI und Protokoll 37, geändert durch den Beschluss des Gemeinsamen EWR-Ausschusses Nr. 154/2018 vom 6. Juli 2018¹,

gestützt auf das Urteil des Gerichtshofs der Europäischen Union in der Rechtssache C-311/18, Data Protection Commissioner/Facebook Ireland Ltd und Maximillian Schrems, vom 16. Juli 2020,

gestützt auf die Empfehlungen 01/2020 des EDSA zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten vom 18. Juni 2021,

gestützt auf die Artikel 10 und 22 seiner Geschäftsordnung,

in Erwägung nachstehender Gründe:

(1) Die wesentliche Aufgabe des Europäischen Datenschutzausschusses (im Folgenden „**EDSA**“) ist die Sicherstellung der einheitlichen Anwendung der DSGVO im gesamten EWR. Zu diesem Zweck ergibt sich aus Artikel 64 Absatz 1 Buchstabe f DSGVO, dass der EDSA eine Stellungnahme abgibt, wenn eine zuständige Aufsichtsbehörde beabsichtigt, verbindliche interne Datenschutzvorschriften (binding corporate rules, im Folgenden „**BCR**“) im Sinne des Artikels 47 DSGVO anzunehmen.

(2) Der EDSA begrüßt und würdigt die Bemühungen der Unternehmen, die DSGVO-Standards in einem globalen Umfeld einzuhalten. Aufbauend auf den Erfahrungen mit der Richtlinie 95/46/EG bekräftigt der EDSA die wichtige Rolle von BCR für internationale Datenübermittlungen sowie seine Zusage, die Unternehmen bei der Gestaltung ihrer BCR zu unterstützen. Diese Stellungnahme dient der Umsetzung dieses Ziels und trägt der Tatsache Rechnung, dass mit der DSGVO das Schutzniveau erhöht wurde, was in den Anforderungen des Artikels 47 DSGVO zum Ausdruck kommt, und dem EDSA die Aufgabe übertragen wurde, zu Entwürfen von Beschlüssen der zuständigen Aufsichtsbehörde zur Genehmigung von BCR eine Stellungnahme abzugeben. Diese Aufgabe des EDSA zielt darauf ab, die einheitliche Anwendung der DSGVO, auch durch Aufsichtsbehörden, Verantwortliche und Auftragsverarbeiter, sicherzustellen.

(3) Nach Artikel 46 Absatz 1 DSGVO darf ein Verantwortlicher oder ein Auftragsverarbeiter, falls kein Beschluss nach Artikel 45 Absatz 3 DSGVO vorliegt, personenbezogene Daten an ein Drittland oder eine internationale Organisation nur übermitteln, sofern der Verantwortliche oder der Auftragsverarbeiter geeignete Garantien vorgesehen hat und sofern den betroffenen Personen

¹ Soweit in dieser Stellungnahme auf „Mitgliedstaaten“ Bezug genommen wird, ist dies als Bezugnahme auf „EWR-Mitgliedstaaten“ zu verstehen.

durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen. Eine Unternehmensgruppe oder eine Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausübt, kann solche Garantien durch die Anwendung rechtsverbindlicher BCR bieten, die den betroffenen Personen ausdrücklich durchsetzbare Rechte übertragen und eine Reihe von Anforderungen erfüllen (Artikel 46 DSGVO). Die Umsetzung und Annahme von BCR durch eine Unternehmensgruppe soll Garantien bieten, die einheitlich in allen Drittländern und folglich unabhängig von dem in den einzelnen Drittländern garantierten Schutzniveau gelten. Die in der DSGVO aufgeführten spezifischen Anforderungen sind diejenigen, die in den BCR mindestens enthalten sein müssen (Artikel 47 Absatz 2 DSGVO). Die BCR müssen von der zuständigen Aufsichtsbehörde (im Folgenden **„federführende Aufsichtsbehörde für BCR“**) nach dem Kohärenzverfahren gemäß Artikel 63 und Artikel 64 Absatz 1 Buchstabe f DSGVO angenommen werden, sofern sie die in Artikel 47 DSGVO festgelegten Bedingungen sowie die Anforderungen, die in den einschlägigen, vom EDSA gebilligten Arbeitsdokumenten der Artikel-29-Datenschutzgruppe² festgelegt sind, erfüllen.

(4) Diese Stellungnahme bezieht sich nur auf die Einschätzung des EDSA, dass die für die vorgeschriebene Stellungnahme vorgelegten BCR insofern angemessene Garantien bieten, als dass sie alle in Artikel 47 DSGVO und dem vom EDSA gebilligten Arbeitsdokument WP 257 rev.01 der Artikel-29-Datenschutzgruppe³ enthaltenen Anforderungen erfüllen. Dementsprechend beziehen sich diese Stellungnahme und die Überprüfung durch die Aufsichtsbehörden in Bezug auf die in den fraglichen BCR behandelten Elemente und Verpflichtungen der DSGVO ausschließlich auf diejenigen, die Artikel 47 DSGVO betreffen. Dies gilt auch für alle ergänzenden Maßnahmen, die ein der DSGVO unterliegender Datenexporteur je nach den Umständen der Übermittlung gegebenenfalls ergreifen muss, um die Einhaltung der in den BCR eingegangenen Verpflichtungen zu gewährleisten.

(5) Der EDSA erinnert daran, dass es nach dem Urteil des Gerichtshofs der Europäischen Union in der Rechtssache C-311/18 dem der DSGVO unterliegenden Datenexporteur obliegt, erforderlichenfalls mit Unterstützung des Datenimporteurs zu beurteilen, ob das vom EU-Recht geforderte Schutzniveau in dem betreffenden Drittland eingehalten wird, um festzustellen, ob die durch die BCR gebotenen Garantien in der Praxis eingehalten werden können, wobei der mögliche Eingriff in die Grundrechte durch die Rechtsvorschriften des Drittlandes zu berücksichtigen ist. Ist dies nicht der Fall, sollte der der DSGVO unterliegende Datenexporteur, erforderlichenfalls mit Unterstützung des Datenimporteurs, prüfen, ob er ergänzende Maßnahmen ergreifen kann, um ein Schutzniveau zu gewährleisten, das dem in der EU der Sache nach gleichwertig ist.

(6) Das vom EDSA gebilligte Arbeitsdokument WP 257 rev.01 der Artikel-29-Datenschutzgruppe enthält die Elemente, die in den BCR für Auftragsverarbeiter (Binding Corporate Rules for Processors, im Folgenden **„BCR-P“**) enthalten sein müssen, einschließlich des Antragsformulars und gegebenenfalls der unternehmensinternen Vereinbarung. Das vom EDSA gebilligte Arbeitsdokument WP 265 der Artikel-29-Datenschutzgruppe⁴ enthält Empfehlungen an die Antragsteller, die

² Die durch Artikel 29 der Richtlinie 95/46/EG eingesetzte Arbeitsgruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten.

Artikel-29-Datenschutzgruppe, Arbeitsdokument mit einer Übersicht über die Bestandteile und Grundsätze verbindlicher interner Datenschutzvorschriften für Auftragsverarbeiter, zuletzt überarbeitet und angenommen am 6. Februar 2018, WP 257 rev.01.

⁴ Artikel-29-Datenschutzgruppe, Empfehlungen zum Standardantrag auf Genehmigung verbindlicher interner Datenschutzvorschriften für Auftragsverarbeiter über die Übermittlung personenbezogener Daten, angenommen am 11. April 2018, WP 265.

veranschaulichen, wie die in Artikel 47 DSGVO und im Arbeitsdokument WP 257 rev.01 enthaltenen Anforderungen erfüllt werden können. Ferner weist der EDSA darauf hin, dass alle eingereichten Unterlagen Gegenstand von Anträgen auf Zugang zu Dokumenten gemäß den nationalen Rechtsvorschriften der zuständigen Aufsichtsbehörden und der Verordnung (EG) Nr. 1049/2001⁵ sein können, die gemäß Artikel 76 Absatz 2 DSGVO für den EDSA gilt.

(7) Angesichts der besonderen Merkmale von BCR gemäß Artikel 47 Absätze 1 und 2 DSGVO sollte jeder Antrag einzeln geprüft werden und hat keine Auswirkung auf die Bewertung anderer BCR. Der EDSA weist darauf hin, dass BCR individuell so angepasst werden sollten, dass sie der Struktur der Gruppe von Unternehmen, für die sie gelten, der von diesen Unternehmen vorgenommenen Verarbeitung und den von ihnen zum Schutz personenbezogener Daten angewandten Strategien und Verfahren Rechnung tragen⁶.

(8) Gemäß Artikel 64 Absatz 3 DSGVO in Verbindung mit Artikel 10 Absatz 2 der Satzung des EDSA hat die Annahme der Stellungnahme des EDSA binnen acht Wochen, nachdem der Vorsitz beschlossen hat, dass die Akte abgeschlossen ist, zu erfolgen. Diese Frist kann unter Berücksichtigung der Komplexität der Angelegenheit auf Beschluss des Vorsitzes des EDSA um weitere sechs Wochen verlängert werden —

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

1 ZUSAMMENFASSUNG DES SACHVERHALTS

1. Im Einklang mit dem im Arbeitsdokument WP 263 rev.01 festgelegten Verfahren der Zusammenarbeit wurde der Entwurf der BCR-P der Cerner Health Services Deutschland GmbH und der teilnehmenden Unternehmen der Gruppe (im Folgenden „**Cerner-Gruppe**“) von der Aufsichtsbehörde Hessens (Deutschland) als federführender Aufsichtsbehörde für BCR überprüft.
2. Die federführende Aufsichtsbehörde für BCR hat ihren Entwurf eines Beschlusses zu dem Entwurf der BCR-P der Cerner-Gruppe vorgelegt und den EDSA am 24. Oktober 2023 um eine Stellungnahme gemäß Artikel 64 Absatz 1 Buchstabe f DSGVO ersucht. Der Beschluss über den Abschluss der Akte erging am 20. November 2023.

2 BEWERTUNG

3. Der Entwurf der BCR-P der Cerner-Gruppe behandelt jegliche Übermittlung oder Weitergabe personenbezogener Daten innerhalb von Unternehmen der Cerner-Gruppe, die rechtlich durch die BCR gebunden sind, d. h. von einem teilnehmenden Unternehmen der Cerner-Gruppe mit Sitz im Europäischen Wirtschaftsraum (EWR), das als Auftragsverarbeiter oder Unterauftragsverarbeiter im

⁵ Verordnung (EG) Nr. 1049/2001 des Europäischen Parlaments und des Rates vom 30. Mai 2001 über den Zugang der Öffentlichkeit zu Dokumenten des Europäischen Parlaments, des Rates und der Kommission.

⁶ Diese Auffassung vertrat die Artikel-29-Arbeitsgruppe in ihrem am 24. Juni 2008 angenommenen Arbeitsdokument „Setting up a framework for the structure of Binding Corporate Rules“ (Festlegung eines Rahmens für die Struktur verbindlicher interner Datenschutzvorschriften), WP 154.

Auftrag und auf Anweisung eines Kunden mit Sitz im EWR fungiert, an ein teilnehmendes Unternehmen der Cerner-Gruppe in einem Drittland⁷.

4. Zu den Betroffenen gehören Kunden von Cerner (einschließlich Patienten, die Kunden sind), für die Cerner als Auftragsverarbeiter fungiert⁸.
5. Der Entwurf der BCR-P der Cerner-Gruppe wurde nach den vom EDSA festgelegten Verfahren geprüft. Die im EDSA zusammengeschlossenen Aufsichtsbehörden sind zu dem Schluss gelangt, dass der Entwurf der BCR-P der Cerner-Gruppe alle nach Artikel 47 DSGVO und dem Arbeitsdokument WP 257 rev.01 erforderlichen Bestandteile enthält, was mit dem Entwurf des Beschlusses der federführenden Aufsichtsbehörde für BCR, der dem EDSA zur Stellungnahme vorgelegt wurde, übereinstimmt. Daher hat der EDSA keine Bedenken, die behandelt werden müssten.

3 SCHLUSSFOLGERUNGEN

6. In Anbetracht der obigen Ausführungen und der Verpflichtungen, die die Gruppenmitglieder durch die Unterzeichnung der Vereinbarung über die Umsetzung der BCR eingehen werden, ist der EDSA der Ansicht, dass der Entwurf des Beschlusses der federführenden Aufsichtsbehörde für BCR in der vorliegenden Form angenommen werden kann, da der Entwurf der BCR-P der Cerner-Gruppe angemessene Garantien enthält, um sicherzustellen, dass das durch die DSGVO garantierte Schutzniveau für natürliche Personen nicht beeinträchtigt wird, wenn personenbezogene Daten an Gruppenmitglieder mit Sitz in Drittländern übermittelt und von diesen verarbeitet werden. Der EDSA erinnert daran, dass die Genehmigung von BCR durch die federführende Behörde für BCR nicht gleichbedeutend ist mit der Genehmigung bestimmter Übermittlungen personenbezogener Daten, die auf der Grundlage der BCR erfolgen. Dementsprechend darf die Genehmigung von BCR nicht als Genehmigung von Übermittlungen an Drittländer ausgelegt werden, die in den BCR enthalten sind und bei denen ein Schutzniveau, das dem in der EU gewährten Schutzniveau im Wesentlichen gleichwertig ist, nicht gewährleistet werden kann.
7. Schließlich verweist der EDSA auch auf Artikel 47 Absatz 2 Buchstabe k DSGVO und das Arbeitsdokument WP 257 rev.01 und die dort festgelegten Bedingungen, unter denen der Antragsteller die BCR ändern oder aktualisieren kann, einschließlich der Aktualisierung der Liste der an sie gebundenen Gruppenmitglieder.

4 ABSCHLIEßENDE BEMERKUNGEN

8. Diese Stellungnahme ist an die federführende Aufsichtsbehörde für BCR gerichtet und wird gemäß Artikel 64 Absatz 5 Buchstabe b DSGVO veröffentlicht.
9. Nach Artikel 64 Absätze 7 und 8 DSGVO übermittelt die federführende Aufsichtsbehörde für BCR dem Vorsitz ihre Antwort auf diese Stellungnahme innerhalb von zwei Wochen nach Erhalt der Stellungnahme.
10. Die federführende Aufsichtsbehörde für BCR muss dem EDSA ihren endgültigen Beschluss mitteilen, damit dieser ihn gemäß Artikel 70 Absatz 1 Buchstabe y der DSGVO im Register der Beschlüsse in Bezug auf Fragen, die im Rahmen des Kohärenzverfahrens behandelt wurden, erfassen kann.

⁷ Abschnitte 1, 17 und 18 der BCR-P-Leitlinien.

⁸ Abschnitt 17 der BCR-P-Leitlinien.

Für den Europäischen Datenschutzausschuss

Die Vorsitzende

(Anu Talus)