Der Landesbeauftragte für den
DATENSCHUTZ und die
INFORMATIONSFREIHEIT
Rheinland-Pfalz

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit RLP
Postfach 3040 | 55020 Mainz

An alle nicht-öffentlichen Stellen in Rheinland-Pfalz

Hintere Bleiche 34 | 55116 Mainz
Postfach 3040 | 55020 Mainz

Telefon +49 (0) 6131 8920-0
Telefax +49 (0) 6131 8920-299

poststelle@datenschutz.rlp.de
www.datenschutz.rlp.de

Ihr Zeichen	Ihre Nachricht vom	Geschäftszeichen	Telefondurchwahl	Datum
		8.69.09:0006	-231	12.05.2021

Datenschutzkonforme Übermittlung personenbezogener Daten in Drittländer nach dem Schrems II-Urteil

Sehr geehrte Damen und Herren,

der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz ist im Anwendungsbereich der Datenschutz-Grundverordnung (DS-GVO) zuständig gemäß Art. 51 Abs. 1, Art. 55 Abs. 1 DS-GVO i.V.m. § 40 Abs. 1 Bundesdatenschutzgesetz (BDSG) und § 15 Abs. 2 Landesdatenschutzgesetz (LDSG) für die Überwachung der Vorschriften über den Datenschutz bei der Datenverarbeitung nicht-öffentlicher Stellen. Bei mehreren Niederlassungen und in Fällen der grenzüberschreitenden Verarbeitung ergibt sich die Zuständigkeit aus § 40 Abs. 2 BDSG sowie Art. 56 DS-GVO i.V.m. § 19 Abs. 1 BDSG.

Als nicht-öffentliche Stelle übermitteln Sie möglicherweise personenbezogene Daten in einen Staat außerhalb der Europäischen Union (EU) bzw. des Europäischen Wirtschaftsraums (EWR) (in sog. Drittländer) und/oder nutzen Dienste oder Programme von Anbietern aus Drittländern. Dies kann z.B. Daten von Kundinnen und Kunden, aber auch von Beschäftigten Ihres Unternehmens betreffen, wenn diese an Auftragsverarbeiter in einem Drittland oder aber an ein anderes Unternehmen innerhalb der Unternehmensgruppe übermittelt werden. Solche Datenübermittlungen sind jedoch nur dann zulässig, wenn bestimmte Anforderungen im Rahmen der DS-GVO erfüllt sind. So eröffnet die DS-GVO folgende Möglichkeiten einer Übermittlung in ein Drittland:

- Die EU-Kommission hat die Feststellung der Angemessenheit des Datenschutzniveaus im Drittland getroffen – sog. Angemessenheitsbeschluss – (Art. 45 DS-GVO),
- es liegen geeignete Garantien vor (Art. 46 DS-GVO) oder
- es liegt eine Ausnahme für bestimmte Fälle vor (Art. 49 DS-GVO).

Insbesondere auch im Rahmen der Nutzung von IT- und Telekommunikationsdiensten von Anbietern aus Drittländern werden häufig personenbezogene Daten dorthin übertragen, ohne

dass dies auf den ersten Blick ersichtlich ist. Um das Ausmaß und die Praxisrelevanz zu verdeutlichen, seien nur beispielhaft und nicht abschließend folgende Anwendungen genannt:

- Videokonferenzsysteme
- Cloudanwendungen
- E-Mailanwendungen
- Newsletterservices
- Social Media Dienste von Anbietern wie Google, Facebook, WhatsApp, Twitter oder Instagram, deren Anbieter ihren Sitz außerhalb der EU oder des EWR haben
- Websiteanalysetools und Webhoster
- Officeanwendungen
- Dokumentenmanagementsysteme

Besonders praxisrelevant und daher häufig betroffen sind Übermittlungen personenbezogener Daten in die USA. Während diese bis Juli 2020 teilweise auf den EU-US Privacy Shield als Angemessenheitsbeschluss gestützt werden konnten, ist dies nun nicht mehr möglich. Am 16. Juli 2020 hat der Europäische Gerichtshof (EuGH) in einem Grundsatzurteil (C-311/18, sog. Schrems-II-Urteil) den EU-US Privacy Shield für ungültig erklärt, da dieser mit Art. 45 Abs. 1 DS-GVO unvereinbar ist. Gemäß dieser Vorschrift dürfen Übermittlungen personenbezogener Daten in ein Drittland nur dann vorgenommen werden, wenn die Kommission beschlossen hat, dass dieses ein angemessenes – demjenigen der EU der Sache nach gleichwertiges – Schutzniveau bietet.

In Bezug auf die USA hat der EuGH die Angemessenheit des Schutzniveaus unter anderem deswegen verneint, weil geltendes US-amerikanisches Recht (insbesondere Section 702 des Foreign Intelligence Surveillance Act (FISA) und die Executive Order 12.333) es den dortigen Nachrichtendiensten erlaubt, zu Zwecken der Auslandsaufklärung uneingeschränkt und ohne konkretes Überwachungsziel auf personenbezogene Daten auch von Nicht-US-Bürgern zuzugreifen. Weiter stellt der EuGH fest, dass diesen kein wirksamer Rechtsbehelf gegen diese Eingriffe in ihr Recht auf informationelle Selbstbestimmung zur Verfügung steht.

Ich weise gemäß Art. 57 Abs. 1 lit. d DS-GVO ausdrücklich darauf hin, dass Datenübermittlungen in die USA bereits jetzt auf andere Transferinstrumente als den EU-US Privacy Shield gestützt werden müssen, da die Gewährung einer Karenzzeit durch die Aufsichtsbehörden weder durch das Urteil des EuGH noch durch die DS-GVO vorgesehen ist. Beachten Sie, dass es sich auch schon dann um eine Datenübermittlung im Sinne des Kapitel V DS-GVO handelt, wenn Daten, die z.B. in Deutschland gespeichert sind, von einer in einem Drittland befindlichen Person per Fernzugriff aufgerufen werden können.

Die Übermittlung auf der Grundlage von Standardvertragsklauseln oder verbindlichen unternehmensinternen Datenschutzvorschriften (Binding Corporate Rules, „BCR“) ist nur unter bestimmten Voraussetzungen möglich. Zwar hat der EuGH in seinem Schrems-II-Urteil die Gültigkeit der eigentlich verfahrensgegenständlichen Standardvertragsklauseln der EU-Kommission (2010/87/EU) bestätigt. Er hat jedoch auch klargestellt, dass die Verantwortlichen, welche Standardvertragsklauseln verwenden, ihren ihnen daraus erwachsenden Pflichten nachkommen müssen. Sollte sich beispielsweise herausstellen, dass der Datenempfänger im Drittland Gesetzen unterliegt, die ihm die Befolgung der Anweisung des Verantwortlichen in der EU und die Einhaltung seiner vertraglichen Pflichten unmöglich machen, hat der Verantwortliche in der EU das vertraglich begründete Recht, die Datenübermittlung

auszusetzen und/oder vom Vertrag zurückzutreten. Um nicht gegen die Vorschriften der DS-GVO zu verstoßen, muss der Verantwortliche in diesem Fall von diesem Recht Gebrauch machen.

In diesem Zusammenhang benennt der EuGH die Möglichkeit der Ergänzung der Standardvertragsklauseln durch die Vertragsparteien, um in der konkreten Vertragsbeziehung dennoch geeignete Garantien dafür zu schaffen, dass das durch die DS-GVO verbürgte Schutzniveau für natürliche Personen nicht beeinträchtigt wird. Dasselbe gilt für die häufig in multinationalen Unternehmensgruppen zum Einsatz kommenden BCR, die ebenfalls nach wie vor grundsätzlich ein geeignetes Transferninstrument darstellen, jedoch nur dann, wenn auch dort den oben formulierten Anforderungen Rechnung getragen wird.

Ausdrücklich betont sei darüber hinaus, dass sich die hier beschriebene Problematik nicht auf Übermittlungen in die USA beschränkt, sondern jegliche Übermittlungen in Drittländer betrifft. Aus diesem Grunde rate ich dringend dazu, alle in Ihrem Unternehmen bzw. Ihrer Organisation stattfindenden Datenverarbeitungsvorgänge im Zusammenhang mit Drittländern anhand des von meiner Behörde bereitgestellten Prüfschemas auf ihre Zulässigkeit hin zu überprüfen und eventuellen Handlungsbedarf zu identifizieren, um Datenschutzverstöße schnellst möglich abzustellen oder zu verhindern. Inwieweit ergänzende Maßnahmen zur Schaffung geeigneter Garantien für ein angemessenes Schutzniveau beitragen können, hat der Europäische Datenschutzausschuss in seinen Empfehlungen 01/2020 dargelegt. Der LfDI weist ausdrücklich darauf hin, dass es Aufgabe des Verantwortlichen ist, Datenverarbeitungsvorgänge datenschutzkonform zu gestalten und die erforderlichen Anstrengungen hierfür zu unternehmen.

Möglicherweise lassen sich bestehende Verarbeitungsprozesse durch ergänzende Maßnahmen nicht in der erforderlichen Weise anpassen. In diesen Fällen kann das Ausweichen auf Anbieter in der EU oder dem EWR unter Umständen die einzige datenschutzkonforme Lösung sein.

Weitere Informationen zu allen oben genannten Aspekten finden Sie auf der Internetseite meiner Behörde: https://www.datenschutz.rlp.de/de/themenfelder-themen/schrems-ii/

Ich beabsichtige, meiner Aufsichtspflicht im Wege stichprobenartiger Überprüfungen nachzukommen. Insbesondere deshalb, aber auch aufgrund der ohnehin bestehenden Rechenschaftspflicht des Verantwortlichen gem. Art. 5 Abs. 2 DS-GVO, empfehle ich dringend, eine Dokumentation der erfolgten Analysen, Bewertungen, Datenschutz-Folgenabschätzungen und der auf Grundlage dessen getroffenen Entscheidungen vorzunehmen.

Bereits jetzt weise ich darauf hin, dass ich im Falle einer unrechtmäßigen Datenübermittlung verpflichtet bin, die Aussetzung des Datentransfers anzuordnen oder diesen gänzlich zu untersagen. Unabhängig davon bin ich jederzeit verpflichtet, etwaigen Beschwerden über mögliche Datenschutzverstöße durch Verantwortliche oder Auftragsverarbeiter mit Sitz oder

Hauptniederlassung in Rheinland-Pfalz nachzugehen.

Mit freundlichen Grüßen

Prof. Dr. Dieter Kugelmann