PfälzischeRechtsanwaltsKammer
Zweibrücken

Kammer-Rundschreiben 5/2021

Zweibrücken, den 16. Juni 2021

Sehr geehrte Damen und Herren Kolleginnen und Kollegen,

das nachfolgende Kammer-Rundschreiben 5/2021 finden Sie auch auf der Kammer-Homepage als PDF-Datei.

I. Datenschutz

1) 28. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz und die Informationsfreiheit zum Datenschutz 2019

Das rheinland-pfälzische Justizministerium hat die Kammer darum gebeten, die in ihrem Zuständigkeitsbereich zugelassenen Rechtsanwältinnen und Rechtsanwälte für die im Bericht des Landesbeauftragen für Datenschutz und Informationsfreiheit Rheinland-Pfalz angesprochene und nachfolgende wiedergegebene Thematik zu sensibilisieren:

„Die häufigste Meldung von Verletzungen nach Art. 33 DS-GVO bzw. § 54 LDSG im Justizbereich betraf den Versand von Dokumenten durch Rechtsanwälte und Notare an unberechtigte Empfänger, etwa durch falsche Eingabe einer E-Mail-Adresse. Die E-Mails wurden in der Regel unverschlüsselt versandt, so dass teilweise sensible Informationen an die falsche Adresse gerieten. Verantwortliche sind nach Art. 24 Abs. 1 und Art. 32 DS-GVO verpflichtet, geeignete technische und organisatorische Maßnahmen für eine verordnungskonforme Verarbeitung zu treffen. Die Verschlüsselung ist in Art. 32 Abs. 1 lit a DS-GVO auch exemplarisch genannt und nach Auffassung des LfDI für vertrauliche E-Mail-Kommunikation geeignet und effektiv. Betrifft die Kommunikation besondere Kategorien personenbezogener Daten nach Art. 9 DS-GVO (wie etwa die ethnische Herkunft, politische Überzeugungen oder Gesundheit) ist die unverschlüsselte Kommunikation besonders kritisch. Sie ist dann allenfalls nach ausdrücklicher vorheriger Einwilligung und Information der betroffenen Personen über die damit verbundenen Risiken möglich. Aber auch bei anderen vertraulichen Daten, wie etwa Finanzdaten oder Eigentumsverhältnisse, sollte die Verschlüsselung der Regelfall sein. Deshalb mahnte der LfDI auch gegenüber Rechtsanwälten und Notaren immer wieder die Verschlüsselung an.“

2) Mit den datenschutzrechtlichen Anforderungen bei der Übermittlung einer E-Mail beschäftigt sich auch das Verwaltungsgericht Mainz mit Urteil vom 17.12.2020 (1 K 778/19.MZ). Nachfolgende die Leitsätze:

   a. Für Streitigkeiten zwischen einer natürlichen oder einer juristischen Person und der Aufsichtsbehörde des Landes über Rechte gemäß Art. 78 Abs. 1 und Abs. 2 DS-GVO ist in Rheinland-Pfalz des Landesbeauftragte für den Datenschutz und die Informationsfreiheit richtiger Beklagter.

   b. Ein angemessenes Schutzniveau im Sinne des Art. 32 Abs. 1 DS-GVO ist auch bei Berufsgeheimnisträgern (hier: Rechtsanwälte) grundsätzlich durch Nutzung einer (obligatorischen) Transportverschlüsselung anzunehmen, soweit nicht im Einzelfall besondere Anhaltspunkte für einen erhöhten Schutzbedarf bestehen.

   Das Urteil des Verwaltungsgerichtes Mainz finden Sie in den BRAK-Mitteilungen 2/2021, Seite 104 bis 111, die auf der Homepage der BRAK zum Download zur Verfügung stehen.

   Bitte beachten Sie aber, dass das Gericht in dem vorliegenden Fall entschieden hatte, dass es sich bei den von dem klagenden Rechtsanwalt übermittelten Informationen nicht um besondere Kategorien personenbezogener Daten nach Art. 9 und 10 DS-GVO (ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetische und biometrische Daten, Gesundheitsdaten, Daten zum Sexualleben oder der sexuellen Orientierung einer Person oder betreffend strafrechtliche Verurteilungen und Straftaten) gehandelt und das Gericht ausschließlich aus diesem Grund eine Ende-zu-Ende-Verschlüsselung nicht für verpflichtend gehalten hat.

3) Datenschutzkonforme Übermittlung personenbezogener Daten in Drittländer nach dem „Schrems II“-Urteil:

   Der rheinland-pfälzische Landesbeauftragte für den Datenschutz und die Informationsfreiheit möchte das Bewusstsein der verarbeitenden Stellen schärfen und damit die Datenschutzrechte der betroffenen Personen, also aller Bürgerinnen und Bürger, stärken und hat die Kammer deshalb darum gebeten, sein nachfolgendes Schreiben an Sie weiterzuleiten:

Der Landesbeauftragte für den
DATENSCHUTZ und die
INFORMATIONSFREIHEIT
Rheinland-Pfalz

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

Hintere Bleiche 34 | 55116 Mainz
Postfach 3040 | 55020 Mainz

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

An alle nicht-öffentlichen Stellen in Rheinland-Pfalz

Ihr Zeichen	Ihre Nachricht vom	Geschäftszeichen	Telefondurchwahl	Datum
		8.69.09:0006		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

Kammer-Rundschreiben 5/2021

II. Geldwäsche

1) Podcast zum Thema Geldwäsche

Am 26.06.2017 ist das neue Geldwäschegesetz (GwG) in Kraft getreten. Das Geldwäschegesetz gibt Rechtsanwälten, wenn sie in Kataloggeschäften nach § 2 Abs. 1 Nr. 10 GwG tätig sind, besondere Pflichten auf. Außerdem obliegt den Rechtsanwaltskammern nun gemäß § 50 Nr. 3 GwG die Präventivaufsicht über die Mitglieder, die nach § 2 Abs. 1 Nr. 10 GwG „Verpflichtete“ sind.

Auf der Homepage der Kammer finden Sie unter dem Reiter „Geldwäschegesetz“ aktuelle Informationen zu den geldwäscherechtlichen Verpflichtungen und dem Aufsichtsverfahren der Kammer.

Die BRAK hat außerdem einen Podcast zum Thema Geldwäsche veröffentlicht, in dem über die Zuständigkeit der Geldwäscheaufsicht, Meldepflichten, richtige Verhaltensweisen und die in Betracht kommenden Sicherungsmaßnahmen informiert wird.

Der Podcast „Geldwäsche – So macht man es richtig“ wurde unter folgendem Link veröffentlicht: https://bundesrechtsanwaltskammer.podigee.io/23-folge.

2) Informationen zur Registrierung für das elektronische Meldeportal goAML der Financial Intelligence Unit

Die FIU hat die Aufsichtsbehörden darum gebeten, die Verpflichteten nach dem GwG über die Registrierungspflicht gemäß § 45 Abs. 1 S.2 GwG durch Veröffentlichung ihres an die Verpflichteten gerichteten Schreibens zu informieren:

Zentralstelle für
Finanztransaktions-
untersuchungen

ZOLL

Generalzolldirektion - FIU, Postfach 85 05 55, 51030 Köln

nur per E-Mail

Verpflichtete nach GwG

GENERALZOLLDIREKTION
Financial Intelligence Unit (FIU)
Direktion X, Fachgebiet A.322
Nationale Zusammenarbeit – Gewerbetreibende und weitere Verpflichtete –

E-MAIL: Registrierung.fiu@zka.bund.de
ANSCHRIFT:
Postfach 85 05 55
51030 Köln
www.fiu.bund.de

DATUM: 31.05.2021

BETREFF **Informationen zur Registrierung für das elektronische Meldeportal goAML Web der Financial Intelligence Unit**

BEZUG --

ANLAGEN --

GZ **SV 6002 - 2021.RUN.800001 - DVIII.D.32**

Sehr geehrte Damen und Herren,

die Zentralstelle für Finanztransaktionsuntersuchungen (Financial Intelligence Unit – FIU) ist die nationale Zentralstelle für die Entgegennahme, Sammlung und Auswertung von Meldungen über verdächtige Finanztransaktionen, die im Zusammenhang mit Geldwäsche oder Terrorismusfinanzierung stehen könnten. Als „Intelligence-Einrichtung“ führt die FIU strategische und operative Analysen der von den Verpflichteten übersendeten Verdachtsmeldungen durch.

Mit Wirkung zum 01.01.2020 wurde das Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten (Geldwäschegesetz – GwG) um wichtige Regelungen ergänzt. Unter anderem wurde mit der Gesetzesänderung auch die Pflicht zur elektronischen Registrierung bei der FIU für Verpflichtete eingeführt und zwar unabhängig von der Abgabe einer Verdachtsmeldung (§ 45 Abs. 1 S. 2 GwG). Hierfür stellt die FIU das elektronische Meldeportal goAML Web zur Verfügung. Die Pflicht zur Registrierung besteht mit Inbetriebnahme des neuen Informationsverbundes der FIU, spätestens jedoch ab dem 01. Januar 2024. Das Bundesministerium der Finanzen gibt den Tag der Inbetriebnahme des neuen Informationsverbundes der Zentralstelle für Finanztransaktionsuntersuchungen im Bundesgesetzblatt bekannt (§ 59 Abs. 6 GwG).

Aus Sicht der FIU ist eine frühzeitige Registrierung in goAML Web empfehlenswert. Insbesondere können Sie sich im Vorfeld mit Ihren Pflichten im Zusammenhang mit der Meldepflicht im Sinne des Geldwäschegesetzes (§§ 43 ff. GwG) befassen, um somit im Bedarfsfall die unverzügliche Abgabe einer Verdachtsmeldung vorzunehmen. Mit der Registrierung in goAML Web erhalten Sie zudem Zugang zu spezifischen Hinweisen und Publikationen der FIU zum Thema Bekämpfung von Geldwäsche und Terrorismusfinanzierung, welche als wichtige Hilfestellungen zur Erfüllung Ihrer geldwäscherechtlichen Verpflichtungen dienen. Ferner zeigt die erfolgreiche Registrierung im Rahmen einer Prüfung durch die zuständige Aufsichtsbehörde, dass Sie sich als Verpflichteter mit dem Thema “Geldwäschebekämpfung“ und den sich aus dem GwG ergebenden Meldepflichten auseinandergesetzt haben.

Abschließend weisen wir Sie auf die Webseite der FIU hin, die das zentrale Informationsportal der FIU darstellt. Hier werden Ihnen u.a. aktuelle Informationen zum Thema „Bekämpfung von Geldwäsche und Terrorismusfinanzierung“ sowie Publikationen zum elektronischen Meldeportal der FIU zur Verfügung gestellt. Nutzen Sie die Möglichkeit des RSS-Feeds, um regelmäßig über neue Inhalte auf der Webseite informiert zu werden.

Bei Fragen zur Registrierung oder zu weiteren Themen rund um die FIU nutzen Sie das Kontaktformular auf der Webseite der FIU oder wenden Sie sich telefonisch an die Servicehotline für Verpflichtete unter +49 (0) 351 / 44834 - 556.

Mit freundlichen Grüßen

Ihre
Financial Intelligence Unit - FIU

PfälzischeRechtsanwaltsKammer
Zweibrücken

Kammer-Rundschreiben 5/2021

III. Sicherheit im Antragsverfahren der Corona-Hilfen

Die BRAK hat darüber informiert, dass sie die technische Möglichkeit geschaffen hat, dass Rechtsanwältinnen und Rechtsanwälte, die für ihre Mandanten Corona-Hilfen beantragen möchten, sich am System einmalig mit ihrer beA-Karte registrieren und auch künftig die beA-Karte für weitere Anmeldungen nutzen können. Dann entfällt die Notwendigkeit, bei fehlender E-Mail-Adresse den per Einschreiben übersandten Code einzugeben.

Zur Verbesserung der Datenqualität wurde außerdem seit Mitte April 2021 ein elektronischer Datenabgleich mit der Finanzverwaltung eingeführt. Damit erfolgt nun bei Antragstellung ein Abgleich der vom Antragsteller angegebenen IBAN mit den beim Finanzamt hinterlegten Daten. Auch dies ist ein wichtiger Schritt auf dem Weg, Betrugsversuche schon bei Antragstellung zu erkennen. Voraussetzung für den elektronischen Datenabgleich ist bei Antragstellung die Angabe der Steuernummer im vereinheitlichten Bundesschema. Dazu ist eine Ausfüllhilfe auf der ELSTER-Website

https://www.elster.de/eportal/helpGlobal?themaGlobal=wo_ist_meine_steuernummer

hinterlegt.

Mit freundlichen kollegialen Grüßen
PFÄLZISCHE RECHTSANWALTSKAMMER

JR Dr. Seither
Präsident

Impressum:
Pfälzische Rechtsanwaltskammer Zweibrücken
Körperschaft des öffentlichen Rechts, vertreten durch ihren Präsidenten
Adresse: Landauer Str. 17, 66482 Zweibrücken
Telefon: 06332/8003-0, Telefax: 06332/800319
E-Mail: zentrale@rak-zw.de, Internet: www.rak-zw.de

Redaktion: Rechtsanwältin Dunja Jahnke, Geschäftsführerin