STIFTUNG DATENSCHUTZ

Schriftliche Stellungnahme zur Anhörung der „Enquetekommission II - Brexit: Auswirkungen auf Nordrhein-Westfalen“ am 10.05.2019

Frage 1: Welche Auswirkungen hat der Brexit auf den Datenschutz im Hinblick auf Datenübermittlungen aus NRW in das VK (und andersherum)?

Antwort 1:

- **Welche Auswirkungen hat der Brexit auf den Datenschutz im Hinblick auf Datenübermittlungen aus NRW in das VK**

Im Falle eines Brexit wird das Vereinigte Königreich zu einem so genannten Drittland: Werden personenbezogene Daten in Länder außerhalb der EU/EWR (so genannte Drittländer/Drittstaaten) übermittelt, darf das Schutzniveau der Datenschutzgrundverordnung nicht unterlaufen werden (Artikel 44 ff. DSGVO – siehe hierzu außerdem die Ausführungen unter 2. und 3.).[1]

Grundsätzlich kann die Sicherstellung eines solchen angemessenen Datenschutzniveaus

- durch einen **Angemessenheitsbeschluss** der Europäischen Kommission (Artikel 45 DSGVO) oder
- durch geeignete **Garantien** herbeigeführt werden (Artikel 46 ff. DSGVO).

Diese **Garantien** (Artikel 46 ff. DSGVO) können in Form von

- *Binding Corporate Rules*
- *Standarddatenschutzklauseln*
- *Verhaltensregeln*
- *Zertifizierungsmechanismen*
- oder *individuellen Vertragsklauseln*

erfolgen.

Anderenfalls ist eine Datenverarbeitung in einem Drittland lediglich unter den Voraussetzungen der in der Datenschutzgrundverordnung abschließend aufgezählten Ausnahmen (Artikel 49 DSGVO) möglich. Solche Ausnahmen können unter anderem aufgrund *wichtiger Gründe des öffentlichen Interesses* oder *wegen des Schutzes lebenswichtiger Interessen* in Betracht kommen, außerdem wenn eine *Einwilligung*

[1] Lediglich zur Klarstellung soll darauf verwiesen werden, dass sich diese Ausführungen auf die Verarbeitung **personenbezogener Daten** von **natürlichen Personen** beziehen. Personenbezogene Daten sind solche Daten, die sich gemäß Artikel 4 Nr. 1 DSGVO auf eine natürliche Person beziehen, z.B. Name, Anschrift, Telefonnummer, Bankdaten, Geburtsdatum, Religionszugehörigkeit, Lichtbilder, etc. Die Definition des Artikel 4 Nr. 1 DSGVO lautet: *„personenbezogene Daten“ sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.*

vorliegt oder *die Übermittlung der personenbezogenen Daten für die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist.*

Die Aufsichtsbehörden vertreten die Auffassung, dass diese Ausnahmen eng auszulegen sind! Daher empfiehlt sich für Verantwortliche stets eine sorgfältige Prüfung dahingehend, ob beispielsweise der Abschluss von Standarddatenschutzklauseln oder Bindung Corporate Rules vorrangig in Betracht kommen muss (siehe hierzu die Ausführungen unter Frage 3).

Insgesamt ist eine „Zwei-Stufen-Prüfung" durchzuführen. Dies bedeutet, dass die Anforderungen der DSGVO gemäß der Kapitel I-IV (1. Stufe) umgesetzt werden müssen, z.B. die Rechtmäßigkeit der Datenübermittlung gemäß Artikel 6 DSGVO. Darüber hinaus müssen auf der zweiten Stufe die in Kapitel V (Artikel 44 ff. DSGVO) niedergelegten Anforderungen an die Übermittlung personenbezogener Daten in Drittländer beachtet werden, dementsprechend - wie oben dargelegt - ein Angemessenheitsbeschluss oder geeignete Garantien vorliegen (siehe hierzu ebenso die Ausführungen unter Frage 3). Diese „Zwei-Stufen-Prüfung" gilt im Übrigen auch für Datenübermittlungen in internationalen Konzernen, da es - wie unter bisherigem Recht - kein Konzernprivileg gibt.[2]

Im umgekehrten Fall verweist die britische Aufsichtsbehörde ICO (Information Commissioner´s Office) darauf, dass im Falle eines Austritts Datenübermittlungen aus dem Vereinigten Königreich in die Europäische Union nicht beschränkt werden.[3] Daher dürfen personenbezogene Daten ohne zusätzliche Bedingungen in die EU übermittelt werden.

- **Besonderheiten für Webseitenbetreiber und Anbieter von Waren und Dienstleistungen**

Insgesamt ist der räumliche Anwendungsbereich gemäß Artikel 3 DSGVO zu beachten, so dass die Datenschutzgrundverordnung für verantwortliche Stellen im Vereinigten Königreich Anwendung finden kann, etwa im Rahmen von Internetangeboten („eCommerce"). So sind ebenso Anbieter von Waren und Dienstleistungen, die personenbezogene Daten von EU-Bürgern verarbeiten, an die Regelungen der DSGVO gebunden. Anderenfalls drohen Sanktionen (Artikel 83 DSGVO), z.B. in Form von Geldbußen. Nach Erwägungsgrund 23 ist entscheidend, ob der Verantwortliche das Anbieten von Waren bzw. Dienstleistungen in der Union „offensichtlich beabsichtigt". Dies liegt vor, wenn die betroffene Person spezifisch angesprochen wird. In diesem Fall muss schriftlich ein Vertreter in der Europäischen Union benannt werden (§ 27 Absatz 1 DSGVO).

Darüber hinaus fällt außerdem jede so genannte Verhaltensbeobachtung in den Anwendungsbereich der DSGVO (Artikel 3 Absatz 2 DSGVO). Damit müssen Webseitenbetreiber, die Cookies verwenden oder Targetingmaßnahmen einsetzen, die Regelungen der DSGVO beachten. Die Datenschutzkonferenz hat in ihrem Positionspapier (vom 26.04.2018) zur Anwendbarkeit des TMG für nicht-öffentliche Stellen dargelegt, dass es beim Einsatz von Tracking-Mechanismen, die das Verhalten von betroffenen Personen im Internet nachvollziehbar machen, einer vorherigen Einwilligung bedarf. Daher ist eine informierte Einwilligung gemäß Artikel 4 Nr. 11 DSGVO und 7 DSGVO in Form einer Erklärung oder sonstigen eindeutig bestätigenden Handlung erforderlich, und zwar bevor Cookies platziert werden.[4]

[2] Erwägungsgrund 48 der DSGVO regelt allerdings für die Datenübermittlung innerhalb einer Unternehmensgruppe, dass hier ein berechtigtes Interesses für interne Verwaltungszwecke, einschließlich der Verarbeitung personenbezogener Daten von Kunden und Beschäftigten, ausreichend sein kann.

[3] Siehe unter https://ico.org.uk/media/for-organisations/documents/brexit/2614575/leaving-the-eu-6-steps-to-take-final.pdf.

[4] Siehe Positionsbestimmung der Datenschutzkonferenz zur Anwendbarkeit des TMG für nicht-öffentliche Stellen vom 26.04.2018, abrufbar unter

An dieser Auffassung hat auch die am 05.04.2019 veröffentlichte Orientierungshilfe für Anbieter von Telemedien der Datenschutzkonferenz nichts geändert.[5] Die Datenschutzkonferenz verweist in ihrer Orientierungshilfe vielmehr darauf, dass eine „unmissverständlich abgegebene Willensbekundung in Form einer Erklärung" beispielweise durch Anklicken eines Kästchens beim Besuch einer Website, durch die Auswahl technischer Einstellungen oder durch eine andere Erklärung oder aktive Verhaltensweise geschehen kann, mit der die betroffene Person eindeutig ihr Einverständnis hinsichtlich der angekündigten und beabsichtigten Datenverarbeitung ausdrückt. Opt-Out-Verfahren reichten dafür nicht aus. Etwas anderes kann nach Auffassung der Datenschutzkonferenz allenfalls bei Tools zur Reichweitenmessung gelten.[6]

Unter Berücksichtigung des räumlichen Anwendungsbereichs der DSGVO führt dies dazu, dass die bloße Zugänglichkeit einer Webseite in der Europäischen Union (auch von Anbietern im Vereinigten Königreich im Falle des Brexit) zur Anwendbarkeit der DSGVO und damit zur Beachtung der gerade genannten Rechtsauffassung führt.[7] Zu berücksichtigen ist hierbei allerdings, dass bei einer in der EU abrufbaren Webseite zu prüfen ist, ob nur eine „gelegentliche" Verarbeitung von personenbezogenen Daten vorliegen könnte, so dass gemäß Artikel 27 Absatz 2 lit. a DSGVO für die Anbieter dann keine Verpflichtung bestehen würde einen Vertreter in der EU zu benennen, wenn die Verarbeitung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt und keine umfangreiche Verarbeitung besonderer Kategorien personenbezogener Daten (z.B. Gesundheitsdaten) oder Daten über strafrechtliche Verurteilungen oder Straftaten stattfindet.

Im Übrigen sind Behörden oder öffentliche Stellen grundsätzlich nicht zur Benennung eines Vertreters in der Europäischen Union verpflichtet (Artikel 27 Absatz 2 lit. b DSGVO).[8]

Frage 2: Welche Folgen entstehen durch die unterschiedlichen Datenschutzniveaus mit dem Vereinigten Königreich (Stichwort: Angemessenheitsbeschluss nach Art. 45 DSGVO)?

Antwort 2:

Eine Datenübermittlung in Drittstaaten darf lediglich erfolgen, wenn das gemäß der DSGVO gewährleistete Schutzniveau für natürliche Personen nicht untergraben wird. Dies kann - wie oben unter 1. dargelegt - unter anderem durch einen Angemessenheitsbeschluss der Europäischen Kommission umgesetzt werden. Dabei muss für jedes Drittland geprüft werden, inwieweit die dort geltenden innerstaatlichen Rechtsvorschriften und Möglichkeiten des gerichtlichen Rechtsschutzes ein der Datenschutzgrundverordnung gleichwertiges Schutzniveau garantieren können. Im Rahmen der Prüfung sind ebenso die Zugriffsmöglichkeit von Sicherheitsbehörden im Vereinigten Königreich auf personenbezogene Daten sowie die Möglichkeiten der Rechtsdurchsetzung durch die Betroffenen zu klären. Die Anerkennung der Angemessenheit eines Datenschutzniveaus ist nur möglich, wenn die Zugriffsmöglichkeiten durch Sicherheitsbehörden begrenzt sind und Bürger der Europäischen Union die

---

https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Technik/Inhalt/TechnikundOrganisation/Inhalt/Zur-Anwendbarkeit-des-TMG-fuer-nicht-oeffentliche-Stellen-ab-dem-25-Mai-2018/Positionsbestimmung-TMG.pdf.

[5] Siehe Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, Stand März 2019, abrufbar unter https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf.

[6] Siehe Fn. 5.

[7] Es wird im Rahmen des räumlichen Anwendungsbereichs allerdings gleichermaßen auf die Probleme der globalen Durchsetzbarkeit in der Praxis verwiesen (Klar in: Kühling/Buchner, DSGVO, Artikel 3 Rn. 26 ff).

[8] Hartung in: Kühling/Buchner, DSGVO, Artikel 27 Rn. 11 verweist darauf, dass es zweifelhaft ist, ob diese Regelung gerechtfertigt sei, da auch ausländische öffentliche Stellen grundsätzlich dem Anwendungsbereich der DSGVO unterfallen können. Er schlägt vor, bei der Begriffsbestimmung danach zu fragen, ob die Verarbeitung zu öffentlichen Zwecken erfolgt.

Möglichkeit haben, Rechtsmittel einzulegen.[9] In diesem Zusammenhang soll beispielhaft auf das Urteil des Europäischen Gerichtshofs vom 6. Oktober 2015 hingewiesen werden, in dem festgestellt wurde, dass die Safe Harbor-Entscheidung der Europäischen Kommission aufgrund der Rechtsordnung in den Vereinigten Staaten und der damit einhergehenden umfassenden staatlichen Überwachung ungültig ist.[10]

⇨ Wenn ein Angemessenheitsbeschluss gemäß Artikel 45 DSGVO bis zum 31.10.2019 vorliegen sollte, dürfen personenbezogene Daten in das Vereinigte Königreich übermittelt werden. Allerdings dauern die Beratungen hierzu an.[11]

Nichtsdestotrotz ist in der praktischen Durchführung zu berücksichtigen, dass die Safe-Harbor-Entscheidung des Europäischen Gerichtshofs dazu geführt hat, dass die europäischen Aufsichtsbehörden auch zukünftig Datenübermittlungen trotz Vorliegen eines Angemessenheitsbeschlusses oder Vorliegen von Standarddatenschutzklauseln (kritisch) im Auge behalten müssen. So liegen zurzeit die bislang geltenden EU-Standardvertragsklauseln im Wege des so genannten Vorabentscheidungsverfahrens dem Europäischen Gerichtshof vor. Nicht ausgeschlossen ist, dass der Europäische Gerichtshof Aussagen zur Zulässigkeit von Datenübermittlungen aufgrund dieser Klauseln trifft, so dass abzuwarten bleibt, inwieweit diese künftig Datenübermittlungen in Drittstaaten rechtfertigen können.

Frage 3: Welche Drittland-Regelungen im Falle eines ungeregelten Austritts sollten aus Landesperspektive befürwortet werden? (Stichwort: Dokumentationspflichten zur Datenübermittlung?)

Antwort 3:

Neben dem unter 2. dargestellten Angemessenheitsbeschluss der Europäischen Kommission sieht die Datenschutzgrundverordnung die Möglichkeit der „geeigneten Garantien" gemäß §§ 46 ff. DSGVO vor, um ein angemessenes Datenschutzniveau sicherzustellen (siehe hierzu oben unter 1.).

Von zentraler Bedeutung ist auch hier, dass den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen müssen!

Im Einzelnen können geeignete Garantien wie folgt umgesetzt werden (deren Vor- und Nachteile sowie Voraussetzungen sind nachfolgend aufgeführt):

- **Verwaltungsvereinbarungen, bilaterale oder multinationale internationale Abkommen für Behörden und öffentliche Stellen**

[9] Roßnagel (Schriftliche Stellungnahme zum öffentlichen Fachgespräch zur Datenschutz-Grundverordnung am 24. Februar 2016 im Ausschuss Digitale Agenda des Deutschen Bundestags, vom 19. Februar 2016) verweist darauf, das sich aus den Passagen des Urteils des Europäischen Gerichtshofs (Safe Harbor Urteil) ergebe, „dass eine Anerkennung der Angemessenheit des Datenschutzniveaus der USA nicht möglich ist; wenn nicht die Zugriffsbefugnisse der US-Sicherheitsbehörden auf das „absolut Notwendige" beschränkt sind und europäische Bürger keine echten Möglichkeiten haben, bei einem Gericht einen wirksamen Rechtsbehelf einzulegen."

[10] Urteil des Europäischen Gerichtshofs vom 6. Oktober 2015, abrufbar unter http://curia.europa.eu/juris/document/document.jsf?docid=169195&mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=DE&cid=703941.

[11] Gemäß der gemeinsamen Informationsveranstaltung des Bundesministeriums des Innern, für Bau und Heimat sowie des Bundesministeriums für Wirtschaft und Energie am 7. März 2019 im Rahmen der Dialogreihe zur Datenschutz-Grundverordnung ist bislang noch kein Angemessenheitsbeschluss erfolgt und die Beratungen und Verhandlungen dauern an.

Öffentliche Stellen (Behörden) können unter den erleichterten Voraussetzungen des Artikel 46 Absatz 2 lit. a DSGVO Datenübermittlungen in Drittstaaten (also auch in das Vereinigte Königreich) vornehmen, sofern den betroffenen Personen durchsetzbare und wirksame Rechte eingeräumt werden. Es muss ein effektiver Rechtsschutz sichergestellt sein, wobei eine solche Rechtsverbindlichkeit im Außenverhältnis nur gewährleistet ist, wenn die genannten Vereinbarungen für die Betroffenen unmittelbar anwendbar sind. Daher bedarf es Kontrollmöglichkeiten durch unabhängige Instanzen, die etwaige Verstöße ermitteln und ahnden können.[12] Bei Vorliegen der Rechtsverbindlichkeit entfällt die Genehmigungspflicht durch eine Aufsichtsbehörde.[13] Nicht rechtlich bindende Verwaltungsvereinbarungen, wie beispielsweise Absichtserklärungen, unterliegen jedoch einer Genehmigungspflicht. So stellt auch der Europäische Datenschutzausschuss klar, dass eine solche Verwaltungsvereinbarung der Genehmigung durch die zuständige nationale Aufsichtsbehörde bedarf, nachdem der Europäische Datenschutzausschuss Stellung genommen hat.[14]

Insgesamt ist also entscheidend, inwieweit die jeweilige Vereinbarung durchsetzbare und effektive Rechte für die betroffenen Personen beinhaltet. So müssen die Betroffenen vor allem ihre Rechte selbst geltend machen können, z.B. über Gerichte. Dies muss daher seitens der öffentlichen Stellen geprüft und umgesetzt werden, sofern als geeignete Garantie und ohne Beteiligung einer Aufsichtsbehörde ein solches Instrument für die Legitimation von Datenübermittlungen gewählt wird.

- **Standarddatenschutzklauseln**

Die Europäische Kommission hat EU-Standardvertragsklauseln zur Sicherstellung eines **angemessenen Datenschutzniveaus** (Datenverarbeitung in Drittstaaten) unter der EU-Richtlinie 95/46/EG veröffentlicht.[15] Diese Regelungen bleiben vorerst in Kraft, es sei denn, die EU-Kommission ersetzt diese durch einen neuen Beschluss. Allerdings verwendet die Datenschutzgrundverordnung nicht mehr den Begriff der „EU-Standardvertragsklauseln" sondern „Standarddatenschutzklauseln". Wie unter bisherigem Recht dürfen diese ohne vorherige Zustimmung der zuständigen Datenschutz-Aufsichtsbehörden verwendet werden, so dass dies grundsätzlich eine einfache Handhabe darstellt, um die Datenverarbeitung in einem Drittstaat zu legitimieren. Der Europäische Datenschutzausschuss betont, dass die Standarddatenschutzklauseln nicht geändert werden dürfen und dass sie so unterzeichnet werden müssen, wie sie von der Europäischen Kommission zur Verfügung gestellt wurden: Diese Regelungen könnten jedoch in einen umfassenderen Vertrag aufgenommen werden und es könnten auch zusätzliche Klauseln verfasst werden und, sofern sie nicht im direkten oder indirekten Widerspruch zu den von der Europäischen Kommission verabschiedeten Standarddatenschutzklauseln stünden.[16]

Unternehmen müssen bei der Verwendung dieser Standarddatenschutzklauseln allerdings berücksichtigen, dass nicht allein der Abschluss eines Vertrages die Angemessenheit des Datenschutzniveaus sicherstellt, sondern (erst) die Umsetzung und Einhaltung der damit verbundenen

[12] Siehe Paal/Pauly, DSGVO, Artikel 46 Rn. 13.
[13] Siehe Artikel 46 Absatz 2 lit. a DSGVO und Erwägungsgrund 108.
[14] Siehe „Information note über Datentransfers im Rahmen der DSGVO im Falle eines No-Deal-Brexits" des Europäischen Datenschutzausschusses, angenommen am 12. Februar 2019, abrufbar unter https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/EDSA_Info_NoDealBrexit_Deutsch__Arbeitsuebersetzung_.pdf.
[15] Diese Standardvertragsklauseln stammen aus den Jahren 2001 und 2004 und 2010 und sind abrufbar unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:181:0019:0031:DE:PDF sowie http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:385:0074:0084:DE:PDF sowie https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32010D0087&from=DE
[16] Siehe „Information note" des Europäischen Datenschutzausschusses, Fn. 14.

Pflichten in der Praxis: Der Empfänger der Daten verpflichtet sich, die Standards des europäischen Datenschutzrechts einzuhalten. Daher soll in diesem Zusammenhang erneut auf die Ausführungen unter Frage 2 hingewiesen werden sowie darauf, dass der Irische High Court deren Rechtswirksamkeit im Wege des Vorabentscheidungsverfahrens vom Europäischen Gerichtshof prüfen lassen möchte.

Dies sollten Unternehmen daher im Auge behalten, sofern sie Datenübermittlungen in Drittstaaten auf der Grundlage der derzeit existierenden EU-Standardvertragsklauseln vornehmen. Nichtsdestotrotz stellen die Vertragsklauseln derzeit eine gültige Rechtsgrundlage dar und können als ein einfach zu handhabendes Instrument dienen, um eine Datenübermittlung zu legitimieren. Hierauf hat ebenso der Europäische Datenschutzausschuss im Rahmen des „letzten Brexittermins" hingewiesen.[17]

- **Binding Corporate Rules**

Geeignete Garantien können außerdem in Form von verbindlichen internen Datenschutzvorschriften (Binding Corporate Rules) erfolgen. Vor allem weltweit tätige Unternehmensgruppen können hiermit ihren internen Datenfluss regeln. Binding Corporate Rules wurden in der Vergangenheit bereits gemäß BDSG-alt angewandt. Der Mindestinhalt ist nun in Artikel 47 Absatz 2 DSGVO klar und konkret festgelegt. Insgesamt müssen die Garantien den nach der Datenschutzgrundverordnung vorgesehenen Schutz widerspiegeln und den betroffenen Personen durchsetzbare Rechte übertragen. Die Genehmigung solcher Binding Corporate Rules erfolgt gemäß dem Kohärenzverfahren durch die zuständige Aufsichtsbehörde. Der Europäische Datenschutzausschuss weist darauf hin, dass sich Organisationen weiterhin auf die unter der früheren Richtlinie 95/46/EG genehmigten Binding Corporate Rules stützen können, da diese unter der DSGVO gültig bleiben.[18] Allerdings müssten diese Binding Corporate Rules im Einklang mit den Bestimmungen der DSGVO aktualisiert werden.[19]

Aufgrund der Genehmigungspflicht durch die zuständige nationale Aufsichtsbehörde ist insgesamt die mögliche Zeitspanne bis zu ihrer endgültigen Geltung zu beachten. In der Praxis wird darauf verwiesen, dass der Genehmigungsprozess sehr lange dauern kann (mehrere Monate oder länger). Zudem ist aktuell die durch DSGVO verursachte Überlastung der Aufsichtsbehörden zu berücksichtigen, so dass nicht ausgeschlossen werden kann, dass Binding Corporate Rules in einigen Fällen nicht mehr rechtzeitig umgesetzt werden können.

- **Genehmigte Verhaltensregeln und genehmigter Zertifizierungsmechanismus**

In der Datenschutzgrundverordnung wurden zudem die Instrumente der genehmigten Verhaltensregeln und des genehmigten Zertifizierungsmechanismus neu eingeführt, um die Verarbeitung von Daten in Drittstaaten zu legitimieren. Darin müssen rechtsverbindliche und durchsetzbare Verpflichtungen des Verantwortlichen oder des Auftragsverarbeiters festgelegt werden, die außerdem seitens der zuständigen Aufsichtsbehörde zu genehmigen sind.

Der Europäische Datenschutzausschuss führt hierzu zwar aus, dass er an Leitlinien arbeitet, die die harmonisierten Bedingungen und Verfahren für die Nutzung dieser Instrumente näher erläutern werden,[20] aber bislang gibt es noch keine Empfehlungen. Die praktische Relevanz dieser beiden

[17] Siehe „Information note" des Europäischen Datenschutzausschusses, Fn. 14.
[18] Siehe „Information note" des Europäischen Datenschutzausschusses, Fn. 14.
[19] Siehe „Information note" des Europäischen Datenschutzausschusses, Fn. 14.
[20] Siehe „Information note" des Europäischen Datenschutzausschusses, Fn. 14.

Instrumentarien bleibt insgesamt abzuwarten. Zudem ist stets die mögliche Zeitdauer bis zu ihrer genehmigten Verwendung in der Praxis mit einzubeziehen.

- **Genehmigte Vertragsklauseln**

Vertragsklauseln, die zwischen dem Verantwortlichen und dem Empfänger der personenbezogenen Daten im Drittland vereinbart wurden, können gleichermaßen die Datenübermittlung unter der Voraussetzung legitimieren, dass die Aufsichtsbehörde diese zuvor genehmigt hat und das Kohärenzverfahren nach Artikel 63 DSGVO durchgeführt wurde.

Daher ist auch hier die möglicherweise lange Zeitspanne bis zu ihrer Genehmigung durch die Aufsichtsbehörde zu berücksichtigen.

Frage 4: Welche Bedenken sollten von Seite des Landes NRW beachtet werden bei Inanspruchnahme von IT-Dienstleistungen durch britische Unternehmen (z.B. Cloud-Lösungen)?

Antwort 4:

Ein Verantwortlicher kann gemäß der Datenschutzgrundverordnung einen Auftragsverarbeitungsvertrag ebenso mit einem Dienstleister abschließen, der seinen Geschäftssitz nicht innerhalb der Europäischen Union hat (z.B. Cloudanbieter), sofern dort ein **angemessenes Datenschutzniveau** vorliegt. Daher gelten die oben unter Nr. 1 bis Nr. 3 gemachten Erwägungen.[21]

Das Instrument der Auftragsverarbeitung ist wie unter dem bisherigen Recht insbesondere für Outsourcing-Verträge relevant. Beispiele sind etwa Verträge im Rahmen von Cloud-Computing, der Newsletterversand, die Auslagerung von Lohn- und Gehaltsabrechnungen oder Backup-Datenspeicherungen.

Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen, wobei Verantwortlicher der Datenverarbeitung nach der Datenschutzgrundverordnung derjenige ist, der allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (Artikel 4 Abs. 7 DSGVO). Der Auftragsverarbeiter ist -wie bisher- ebenso nach den Regelungen der Datenschutzgrundverordnung weisungsgebunden. Im Falle einer gesonderten vorherigen Zustimmung des Verantwortlichen darf ein Auftragsverarbeiter jedoch selbst Subunternehmer unter der Voraussetzung beauftragen, dass diesen dieselben Datenschutzpflichten auferlegt werden und insbesondere hinreichende Garantien hinsichtlich der geeigneten technischen und organisatorischen Maßnahmen vorliegen (siehe hierzu die Regelungen des Artikel 28 Absatz 2 und Absatz 4 DSGVO).

Neu ist, dass die Datenschutzgrundverordnung dem Auftragsverarbeiter mehr Rechtspflichten auferlegt (z.B. Verzeichnis für Verarbeitungstätigkeiten) und zudem Haftungsregelungen bei Datenschutzverletzungen enthält.

Sofern rechtswidrig auf einen Vertrag zur Auftragsverarbeitung verzichtet wird, droht ein Bußgeld bis zu 10 Millionen Euro oder bis zu 2% des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs (Artikel 83 Absatz 4 lit.a i.V.m. Artikel 28 DSGVO).

[21] Nach der Datenschutzgrundverordnung müssen die zusätzlichen Anforderungen der Artikel 44 ff. DSGVO für Verarbeitungen in Drittstaaten eingehalten werden (Angemessenheitsbeschluss gemäß Artikel 45 DSGVO oder geeignete Garantien nach Artikel 46 ff. DSGVO, wie z.B. Standarddatenschutzklauseln).

Insgesamt sind jedoch einzelne Rechtsfragen ungeklärt, etwa die Abgrenzung zur Funktionsübertragung oder die Anwendung auf Fernwartungsverträge. Die Datenschutzkonferenz vertritt die Auffassung, dass IT-Wartungsverträge den Anforderungen des Artikel 28 DSGVO genügen müssen.[22]

In bereits bestehenden Verträgen zur Auftragsverarbeitung muss insgesamt geprüft werden, inwieweit die Anforderungen des Artikel 28 DSGVO bereits enthalten sind. Ansonsten müsste eine Ergänzungsvereinbarung geschlossen werden. Beispielhaft sei hier auf die Regelungen für Subunternehmer verwiesen, so dass die Regelung des Artikel 28 Absatz 2 DSGVO umzusetzen wäre:[23] Nimmt der Auftragsverarbeiter die Dienste eines weiteren Auftragsverarbeiters in Anspruch, so sind diesem im Übrigen dieselben Datenschutzpflichten aufzuerlegen, die in dem Vertrag zwischen dem Verantwortlichen und dem Auftragsverarbeiter festgelegt sind.[24]

Für öffentliche Stellen des Landes Nordrhein-Westfalen, die gemäß § 35 Landesdatenschutzgesetz Nordrhein-Westfalen im Rahmen ihrer Aufgabenwahrnehmung personenbezogene Daten zur Verhütung, Ermittlung, Verfolgung und Ahndung von Straftaten verarbeiten (z.B. Polizeibehörden, Behörden der Finanzverwaltung), stellt § 52 Landesdatenschutzgesetz Nordrhein-Westfalen klar, dass die Rechte der betroffenen Personen auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung und Schadensersatz gegenüber dem Verantwortlichen (der öffentlichen Stelle) geltend gemacht werden und dass außerdem die Regelungen der in der DSGVO geregelten Auftragsverarbeitung entsprechend anzuwenden sind,[25] wenn die Prüfung oder Wartung von automatisierten Verfahren oder Datenverarbeitungsanlagen durch andere Personen oder Stellen im Auftrag vorgenommen wird.

Frage 5: Gibt es Konfliktfelder im Kontext des Schutzes für öffentliche, personenbezogene und/oder unternehmenseigene Daten aus NRW im Zuge des Brexit?

Antwort 5:

Die britische Aufsichtsbehörde ICO (Information Commissioner´s Office) verweist darauf, dass im Falle eines Austritts die Regelungen der DSGVO in nationales Recht integriert werden.[26] Es wurden auch bereits entsprechende gesetzliche Regelungen erlassen.[27] Allerdings beinhalten diese Änderungen und Ergänzungen der Regelungen der DSGVO. Aufgrund der Kürze der Zeit für diese Stellungnahme konnte jedoch keine Prüfung dieser nationalen Regelungen dahingehend erfolgen, inwieweit trotz dieser Änderungen das Datenschutzniveau dem der Datenschutzgrundverordnung entspricht. Zu berücksichtigen ist dennoch der wichtige Punkt, dass eine dem Artikel 48 DSGVO entsprechende Regelung nicht im Gesetz verankert ist. Artikel 48 DSGVO regelt die nach dem Unionsrecht nicht

[22] Siehe Kurzpapier „Auftragsverarbeitung, Artikel 28 DSGVO“ der Datenschutzkonferenz, abrufbar unter https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_13.pdf.

[23] *Der Auftragsverarbeiter nimmt keinen weiteren Auftragsverarbeiter ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen in Anspruch. Im Fall einer allgemeinen schriftlichen Genehmigung informiert der Auftragsverarbeiter den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.*

[24] Ein Vertragsmuster zur Auftragsverarbeitung ist im Übrigen auch beim Bayerischen Landesamt für Datenschutzaufsicht abrufbar.Siehe Bayerisches Landesamt für Datenschutzaufsicht, abrufbar unter https://www.lda.bayern.de/media/muster_adv.pdf.

[25] Unter Verweis auf Artikel 28 Absatz 1 bis 4, 9 und 10, sowie Artikel 29 der Verordnung (EU) 2016/679.

[26] Siehe unter https://ico.org.uk/for-organisations/data-protection-and-brexit/information-rights-and-brexit-frequently-asked-questions/.

[27] Siehe unter http://www.legislation.gov.uk/uksi/2019/419/introduction/made.

zulässige Übermittlung oder Offenlegung von personenbezogenen Daten. Danach darf jegliches Urteil eines Gerichts eines Drittlands und jegliche Entscheidung einer Verwaltungsbehörde eines Drittlands, mit denen von einem Verantwortlichen oder einem Auftragsverarbeiter die Übermittlung oder Offenlegung personenbezogener Daten verlangt wird, nur dann anerkannt oder vollstreckbar werden, wenn sie auf eine in Kraft befindliche internationale Übereinkunft wie etwa ein Rechtshilfeabkommen zwischen dem ersuchenden Drittland und der Union oder einem Mitgliedstaat gestützt sind. Erfasst sind sowohl Urteile von Gerichten als auch Verwaltungsentscheidungen (demnach sämtliche hoheitlichen Akte einer Stelle im Drittland), allerdings keine Herausgabeverlangen von privaten Dritten, selbst wenn diese auf z.B. bei US-Pre-Trial-Discovery-Verfahren im Rahmen eines gerichtlichen Verfahrens erfolgen.[28] Die Übermittlung ist daher insgesamt nur zulässig, wenn diese auf ein internationales Übereinkommen (z.B. Rechtshilfeabkommen) gestützt werden kann. Hier wird etwa auf das Haager Übereinkommen über die Beweisaufnahme im Ausland in Zivil- oder Handelssachen vom 18.03.1970 verwiesen[29] oder das Abkommen zwischen den Vereinigten von Amerika und der Europäischen Union über die Verwendung von Fluggastdatensätzen und deren Übermittlung an das United States Department of Homeland Security vom 14.12.2011.[30]

Sollte das Vereinigte Königreich Artikel 48 DSGVO zukünftig nicht beachten, wäre die Folge, dass damit ein nicht gleichwertiges Schutzniveau verbunden wäre. Dies ist ebenso eine Frage, die von der EU-Kommission im Rahmen ihrer Verhandlungen zu einem Angemessenheitsbeschluss gemäß Artikel 45 DSGVO berücksichtigt werden muss, da damit ein uneinheitliches Schutzniveau im räumlichen Anwendungsbereich der Datenschutzgrundverordnung verbunden wäre. Dies kann aber ebenso Auswirkungen auf mögliche interne Vereinbarungen haben, wie etwa den Abschluss von Binding Corporate Rules oder Vereinbarungen zwischen öffentlichen Stellen. Denn zu beachten ist, dass sowohl verantwortliche Stellen im Vereinigten Königreich personenbezogene Daten an ausländische Behörden und Gerichte auch ohne geltendes Rechtshilfeabkommen übermitteln dürften. Dies müsste daher gleichermaßen eine zuständige Aufsichtsbehörde im Rahmen eines Genehmigungsverfahrens von internen Datenschutzvorschriften berücksichtigen.

Dieser Konfliktfall kann insgesamt sowohl bei einem geregelten als auch ungeregelten Austritt sowie (selbst) bei einem Verbleib des Vereinigten Königreiches in der EU eintreten, da es bereits angekündigt hatte, Artikel 48 DSGVO nicht beachten zu wollen.[31] Um den Grundrechtsschutz der Betroffenen zu gewährleisten, muss daher der freie Datenverkehr mit dem Vereinigten Königreich eingeschränkt werden bzw. sein.[32]

Zu berücksichtigen ist ebenso, dass zwischen dem Vereinigten Königreich und den Vereinigten Staaten (derzeit) mit Austritt aus der EU keine dem Privacy Shield vergleichbare Regelung vorliegt, welche –

[28] Schröder in: Kühling/Buchner, DSGVO, Artikel 48 DSGVO Rn. 13.
[29] Siehe Pauly in: Paal/Pauly, DSGVO, Artikel 48 DSGVO Rn. 8 und mit Verweis auf BGBl. 1977, Teil II Nr. 54, 1452 ff.
[30] Siehe Schröder in: Kühling/Buchner, DSGVO, Artikel 48 Rn. 16 und mit Verweis auf ABl. L. 215/5.
[31] Pauly in: Paal/Pauly, DSGVO, Artikel 48 Rn. 3, Schöder in: Kühling/Buchner, DSGVO, Artikel 48 Rn. 25.
[32] Siehe Roßnagel (Schriftliche Stellungnahme zum öffentlichen Fachgespräch zur Datenschutz-Grundverordnung am 24. Februar 2016 im Ausschuss Digitale Agenda des Deutschen Bundestags, vom 19. Februar 2016), allerdings noch mit Verweis auf Artikel 43a DSGVO, dessen Regelungen nun in Artikel 48 DSGVO enthalten sind: „*Wenn Großbritannien Art. 43a DSVGO nicht anerkennt, muss es den anderen Mitgliedstaaten möglich sein, in ihren Anpassungsgesetzen zur Datenschutz-Grundverordnung den freien Datenverkehr mit Großbritannien aus diesem Grund einzuschränken. Das Verbot des Art. 1 Abs. 3 DSGVO, dass der freie Verkehr personenbezogener Daten in der Union aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt noch verboten werden darf, kann nur gelten, soweit der Grundrechtsschutz durch die in der Verordnung geregelten Schutzklauseln gewährleistet ist.*“

trotz aller Kritik[33]- derzeit die Legitimationsgrundlage für Datenübermittlungen aus europäischen Staaten an Unternehmen in den Vereinigten Staaten darstellt.[34]

Frage 6: Welche öffentlichen Stellen in NRW sind betroffen/ haben Handlungsbedarf?

Antwort 6:

Handlungsbedarf haben grundsätzlich alle öffentlichen und nicht-öffentlichen Stellen, die personenbezogene Daten (z.B. von Beschäftigten (Bewerbern), Kunden oder Nutzern von Onlinediensten) in das Vereinigte Königreich übermitteln oder dort ansässigen Unternehmen Zugriff auf diese Daten gewähren. Dies kann eine Niederlassung im Vereinigten Königreich oder Dienstleister, wie z.B. Cloud-Anbieter, betreffen aber auch andere Auftragnehmer mit Sitz im Vereinigten Königreich.

Unter den Begriff der öffentlichen Stellen können unter anderem Behörden, aber ebenso Hochschulen oder Stiftungen fallen. § 2 Absatz BDSG definiert öffentliche Stellen des Bundes und der Länder als Behörden, Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen. Dies entspricht der Definition gemäß § 5 Datenschutzgesetz Nordrhein-Westfalen. So ist in Bezug auf die öffentlichen Stellen des Landes zu berücksichtigen, dass nicht das BDSG anwendbar ist sondern ausschließlich das Datenschutzgesetz Nordrhein-Westfalen gilt. Allerdings regelt das Datenschutzgesetz Nordrhein-Westfalen die notwendigen ergänzenden Regelungen und spezifische Anforderungen an die Verarbeitung personenbezogener Daten (ausschließlich) innerhalb der Grenzen sowie unter Bezug auf die Verordnung (EU) 2016/679 (DSGVO).

Gemäß Artikel 2 Absatz 2 lit. d DSGVO *findet die Verordnung keine Anwendung auf die Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit.* Außerdem dürfen die Mitgliedstaaten die Verarbeitung personenbezogener Daten durch Gerichte und Justizbehörden näher regeln.[35] Insgesamt ist die zulässige Datenverarbeitung zur Kriminalitätsbekämpfung in den einzelnen Mitgliedstaaten dennoch an den jeweiligen datenschutzrelevanten Grundrechten zu messen und es gilt die Richtlinie (EU) 2016/680.[36] Der Europäische Datenschutzausschuss verweist dementsprechend darauf, dass den

[33] In Bezug auf die Übermittlung von Daten in die USA aufgrund des EU-US Privacy Shield geht der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz davon aus, dass dieses trotz der von den Datenschutzaufsichtsbehörden geäußerten Kritik als Grundlage genutzt werden kann, um personenbezogene Daten aus Europa an solche U.S.-Unternehmen zu transferieren, die sich gemäß dem Privacy Shield zertifiziert haben (https://www.datenschutz.rlp.de/de/themenfelder-themen/privacy-shield/).

[34] Dieser Angemessenheitsbeschluss der Europäischen Kommission gilt einschränkend für Unternehmen in den Vereinigten Staaten, die sich verpflichtet haben, den Datenschutzstandard des Privacy Shield einzuhalten. Siehe Bekanntmachung C(2016) 4176 final zum EU-US Privacy Shield, abrufbar unter https://www.ftc.gov/system/files/documents/plain-language/annexes_eu-us_privacy_shield_en1.pdf sowie DURCHFÜHRUNGSBESCHLUSS (EU) 2016/1250 DER KOMMISSION vom 12. Juli 2016, gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes (bekannt gegeben unter Aktenzeichen C(2016) 4176, abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016D1250&from=DE).

[35] So regelt Erwägungsgrund 20: „*Diese Verordnung gilt zwar unter anderem für die Tätigkeiten der Gerichte und anderer Justizbehörden, doch könnte im Unionsrecht oder im Recht der Mitgliedstaaten festgelegt werden, wie die Verarbeitungsvorgänge und Verarbeitungsverfahren bei der Verarbeitung personenbezogener Daten durch Gerichte und andere Justizbehörden im Einzelnen auszusehen haben. Damit die Unabhängigkeit der Justiz bei der Ausübung ihrer gerichtlichen Aufgaben einschließlich ihrer Beschlussfassung unangetastet bleibt, sollten die Aufsichtsbehörden nicht für die Verarbeitung personenbezogener Daten durch Gerichte im Rahmen ihrer justiziellen Tätigkeit zuständig sein.*“

[36] Siehe hierzu auch Ernst in: Paal/Pauly, Artikel 2 DSGVO Rn. 22.

Behörden, die Strafverfolgungsfunktionen wahrnehmen, zusätzliche Übermittlungsinstrumente zur Verfügung stehen.[37] Er nimmt hierbei Bezug auf Funktionen, die in den Geltungsbereich der Richtlinie (EU) 2016/680 fallen und weist auf Artikel 37 und 38 dieser Richtlinie hin, gemäß derer z.B. Datentransfers stattfinden könnten, wenn die EU-Behörde nach einer (Selbst-) Bewertung aller mit der Übermittlung verbundenen Umstände zu dem Schluss komme, dass in einem Drittland geeignete Garantien bestünden. [38] Darüber hinaus könnten außerdem zusätzliche Ausnahmeregelungen für bestimmte Situationen vorgesehen werden, wobei der Europäische Datenschutzausschuss diesbezüglich Artikel 38 der Richtlinie (EU) 2016/680 aufführt.[39]

In diesem ist in § 29 Polizeigesetz des Landes Nordrhein-Westfalen geregelt, dass eine Übermittlung personenbezogener Daten an Drittländer durch die Polizei zulässig ist, soweit dies zur Erfüllung polizeilicher Aufgaben, zur Abwehr erheblicher Gefahr oder dafür erforderlich ist, dass die Begehung von Straftaten von erheblicher Bedeutung verhindert wird. In Bezug auf Ordnungswidrigkeiten regelt § 64 Datenschutzgesetz Nordrhein-Westfalen i.V.m § 35 Datenschutzgesetz Nordrhein-Westfalen, dass die Übermittlung von personenbezogenen Daten auch ohne geeignete Garantien an Drittländer möglich ist, wenn Ordnungswidrigkeiten verhütet, ermittelt, aufgedeckt, verfolgt oder geahndet werden sollen. An dieser Stelle soll daher ergänzend darauf hingewiesen werden, dass vom Anwendungsbereich des § 35 Absatz 2 Datenschutzgesetz Nordrhein-Westfalen gleichermaßen Ordnungsbehörden erfasst sein sollen, soweit sie Ordnungswidrigkeiten verfolgen, ahnden sowie Sanktionen vollstrecken. Die §§ 35 ff. Datenschutzgesetz Nordrhein-Westfalen dienen der Umsetzung der Richtlinie (EU) Nr. 2016/680, die sich (jedoch) auf Straftaten bezieht. Gemäß Erwägungsgrund 13 der Richtlinie (EU) Nr. 2016/680 ist eine Straftat im Sinne dieser Richtlinie ein eigenständiger Begriff des Unionsrechts, der durch den Gerichtshof der Europäischen Union auszulegen ist. Insgesamt ist umstritten, ob sich der Anwendungsbereich der Richtlinie (EU) Nr. 2016/680 auch auf die Verfolgung von Ordnungswidrigkeiten bezieht.[40] So wird vertreten, dass das Ordnungswidrigkeitsverfahren weitgehend dem Strafverfahren nachgebildet ist, so dass wegen der Einheit der Rechtsordnung die Verfolgung von Ordnungswidrigkeiten in den Anwendungsbereich der Richtlinie fallen soll.[41] Außerdem wird darauf verwiesen, dass nicht alle EU-Mitgliedstaaten über ein dem deutschen Ordnungswidrigkeitenrecht vergleichbares Recht der Verwaltungssanktionen verfügen und daher der Straftatenbegriff auch Ordnungswidrigkeiten mit einschließen müsse.[42] Zu beachten ist dennoch, dass durch die Richtlinie (EU) Nr. 2016/680 das informationelle Selbstbestimmungsrecht stärker eingeschränkt werden kann als nach den Grundsätzen der Datenschutzgrundverordnung. Bei ihrer Anwendung auf Behörden, denen die Ahndung und Verfolgung von Ordnungswidrigkeiten zugewiesen ist, ist damit eine Beschränkung der Rechte der Betroffenen verbunden (da diese Richtlinie andere Zwecke und Ziele verfolgt als die Datenschutzgrundverordnung). So liegt vor allem ein Ungleichgewicht zwischen Ordnungswidrigkeiten und Straftaten vor, da einer Ordnungswidrigkeit kein Strafcharakter zukommt und das Bußgeldverfahren geringere Bedeutung hat. In diesem Zusammenhang ist außerdem darauf hinzuweisen, dass gemäß § 35 Absatz 2 Datenschutzgesetz Nordrhein-Westfalen ebenso die

[37] Siehe „Information note“ des Europäischen Datenschutzausschusses, Fn. 14.
[38] Siehe „Information note“ des Europäischen Datenschutzausschusses, Fn. 14.
[39] Siehe „Information note“ des Europäischen Datenschutzausschusses, Fn. 14.
[40] Auf diesen Streitpunkt ist die Verfasserin ebenso in ihrer schriftlichen Stellungnahme zur Anhörung zum Gesetzentwurf des Hessischen Gesetzes zur Anpassung Hessischen Datenschutzrechts an die Verordnung (EU) Nr. 2016/679 und zur Umsetzung der Richtlinie (EU) Nr. 2016/680 und zur Informationsfreiheit vom 08.03.2018 eingegangen.
[41] Siehe etwa Landesbeauftragte für den Datenschutz Niedersachsen, abrufbar unter https://www.lfd.niedersachsen.de/startseite/datenschutzreform/richtlinie_justiz_inneres_jirichtlinie/
[42] Hörauf, ZIS 2013, S. 276 ff., 278 ff.

Datenverarbeitung kommunaler Ordnungsbehörden im Kontext der Einleitung und Durchführung von Bußgeldverfahren unter den Anwendungsbereich der Richtlinie (EU) Nr. 2016/680 fallen würde.

- **Regelungen des Datenschutzgesetzes Nordrhein-Westfalen in Bezug auf Datenübermittlungen für Zwecke der Verfolgung von Straftaten und Ordnungswidrigkeiten:**

Bei einer Datenübermittlung in Drittstaaten gelten für die in § 35 Datenschutzgesetz Nordrhein-Westfalen genannten öffentlichen Stellen (**Polizeibehörden, Gerichte in Strafsachen und die Staatsanwaltschaften, Strafvollstreckungs- und Justizvollzugsbehörden, Behörden des Maßregelvollzugs, Behörden der Finanzverwaltung und Ordnungsbehörden, soweit sie Ordnungswidrigkeiten verfolgen, ahnden sowie Sanktionen vollstrecken**) insgesamt die Regelungen der §§ 62 ff. Datenschutzgesetz Nordrhein-Westfalen. Diesbezüglich ist wie folgt zu unterteilen:

- Liegt ein **Angemessenheitsbeschluss** (in Bezug auf einen Drittstaat, etwa Großbritannien) vor, so gilt § 62 Datenschutzgesetz Nordrhein-Westfalen: Die verantwortliche Stelle muss - trotz Angemessenheitsbeschluss - zusätzlich beurteilen, ob in dem Drittstaat ein datenschutzrechtlich angemessener und die elementaren Menschenrechte wahrender Umgang mit den Daten beim Empfänger gesichert ist. Die verantwortliche Stelle muss außerdem sicherstellen, dass der Empfänger die übermittelten Daten nur dann an andere Drittstaaten weiterübermittelt, wenn sie diese Übermittlung zuvor genehmigt hat. Personenbezogene Daten, die aus einem anderen Mitgliedstaat der Europäischen Union übermittelt werden, dürfen nur dann in einen Drittstaat übermittelt werden, wenn die zuständige Stelle des anderen Mitgliedstaates diese Übermittlung zuvor genehmigt hat.

- Liegt **kein Angemessenheitsbeschluss** (in Bezug auf einen Drittstaat, etwa Großbritannien) vor, ist die Übermittlung personenbezogener Daten in einen Drittstaat unter den Voraussetzungen des § 63 Datenschutzgesetz Nordrhein-Westfalen möglich. Hierfür müssen entweder geeignete Garantien vorliegen, die in einem rechtsverbindlichen „Instrument“ (z.B. Dokument) geregelt sein können, oder die verantwortliche Stelle muss nach Beurteilung aller Umstände zur Auffassung gelangen, dass geeignete Garantien für den Schutz personenbezogener Daten bestehen. Letzteres entspricht den Ausführungen des Europäischen Datenschutzausschusses, gemäß derer Strafverfolgungsbehörden zusätzliche Übermittlungsbefugnisse zukommen können und dass den Behörden, die Strafverfolgungsfunktionen wahrnehmen, im Sinne der Richtlinie (EU) Nr. 2016/680 eine eigenständige Bewertungskompetenz dafür zukommen kann, ob geeignete Garantien im Drittstaat vorliegen. Allerdings ist - wie oben bereits geschildert - zu berücksichtigen, dass diese Einschränkung der Betroffenenrechte gemäß des Datenschutzgesetzes Nordrhein-Westfalen ebenso durch Ordnungsbehörden im Zusammenhang mit der Verfolgung von Ordnungswidrigkeiten möglich ist.

- Entsprechendes gilt auch im Rahmen der Datenübermittlung an Drittstaaten gemäß § 64 oder § 65 Datenschutzgesetz Nordrhein-Westfalen. § 64 Datenschutzgesetz Nordrhein-Westfalen regelt die Datenübermittlung ohne geeignete Garantien, die unter anderem zulässig sein soll, wenn diese unter Abwägung der Grundrechte der betroffenen Person mit dem öffentlichen Interesse an der Übermittlung für die Zwecke des § 35 Datenschutzgesetz Nordrhein-Westfalen (also etwa zur Verfolgung und Ahndung von Straftaten oder Ordnungswidrigkeiten) erforderlich ist. § 65 Datenschutzgesetz Nordrhein-Westfalen regelt, dass die Datenübermittlung darüber hinaus an Stellen in Drittstaaten übermittelt werden dürfen, die Daten nicht zum Zwecke der Verhütung, Ermittlung, Verfolgung und Ahndung von Straftaten

oder Ordnungswidrigkeiten oder zur Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung verarbeiten. Insoweit schaffen die Regelungen der §§ 62 ff. Datenschutzgesetz Nordrhein-Westfalen für die Polizei- und Ordnungsbehörden weitreichende Befugnisse im Hinblick auf Datenübermittlungen in Drittstaaten.

Ansonsten ist für **Ordnungsbehörden** die Regelung des § 24 Absatz 2 Ordnungsbehördengesetz (OBG) Nordrhein-Westfalen anwendbar. Danach gilt die Verarbeitung personenbezogener Daten durch die Ordnungsbehörden zur Erfüllung ihrer Aufgaben nach diesem Gesetz die Datenschutzgrundverordnung und ergänzend Teil 1 und Teil 2 des Datenschutzgesetzes Nordrhein-Westfalen. Dementsprechend dürften Ordnungsbehörden Daten in Drittstaaten lediglich unter den Voraussetzungen der §§ 44 ff. DSGVO übermitteln. Letzteres hat ebenso Auswirkung auf die bereits unter 5. behandelte Frage der Anwendbarkeit von Artikel 48 DSGVO, und zwar dahingehend unter welchen Voraussetzungen Datenübermittlungen an Gerichte oder Behörden in Drittländern gerechtfertigt sein können, die unter den Anwendungsbereich der DSGVO fallen. Sofern man die Auffassung vertritt, dass Artikel 48 DSGVO als eine abschließende Regelung betrachtet werden sollte,[43] dürften auch öffentliche Stellen personenbezogene Daten lediglich an Gerichte oder Behörden übermitteln, wenn ein entsprechendes Rechtshilfeabkommen vorliegt. Dies würde sich auf Datenverarbeitungen der Polizei und Verwaltungsbehörden im Zusammenhang mit dem Schutz privater Rechte oder auf die Gefahrenabwehr durch Ordnungsbehörden beziehen, sofern hier der Anwendungsbereich der Datenschutzgrundverordnung zugrunde gelegt wird. In diesem Zusammenhang müsste demnach die nicht einfach zu beantwortende Frage nach der Reichweite des Anwendungsbereichs Richtlinie (EU) Nr. 2016/680 entschieden werden.

Frage 7: Welche wichtigen Unterschiede würden die versch. Brexit-Szenarien für NRW im Kontext des Datenschutzes ergeben (Stichwort: Datenschutzgrundverordnung in Verbindung mit dem Bundesdatenschutzgesetz-2018)?

Antwort 7:

Unter der Voraussetzung, dass das Vereinigte Königreich dem Austrittsabkommen noch bis zum 31.10.2019 zustimmt, sind die Regelungen der Artikel 71, 73 sowie 126 relevant.[44] Artikel 126 des (bisherigen) Austrittsabkommens regelt eine Übergangsfrist bis zum 31.12.2020. Danach soll Unionsrecht für die Verarbeitung der personenbezogenen Daten außerhalb des Vereinigten Königreichs gelten, sofern diese vor dem 31.12.2020 im Vereinigten Königreich gemäß Unionsrecht verarbeitet wurden oder nach dem 31.12.2020 auf Basis des Austrittabkommens verarbeitet werden. Diese Regelung soll nur dann nicht (mehr) gelten, sofern ein Angemessenheitsbeschluss gemäß Artikel 45 DSGVO vereinbart wird (Artikel 71 Absatz 2 des Austrittsabkommens), wobei das Vereinigte Königreich auch ohne einen solchen Angemessenheitsbeschluss einen Schutz personenbezogener Daten gewährleisten möchte, der dem Schutzniveau des Unionsrechts im Wesentlichen entspricht (Artikel 71 Absatz 3 des Austrittsabkommens). Weiterhin ist geregelt, dass die EU Daten aus dem Vereinigten Königreich, die es vor dem Ablauf des Übergangszeitraums oder die es nach dem Ablauf des Übergangszeitraums aufgrund dieses Abkommens erhalten hat, nicht anders als Daten aus anderen Mitgliedstaaten behandelt. Der Austritt aus der Union soll für diesen Fall unerheblich sein (Artikel 73

[43] Siehe hierzu Schröder in: Kühling/Buchner, DSGVO, Artikel 48 Rn. 22 ff.

[44] Draft Agreement on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community14 November 2018 - https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/756374/14_November_Draft_Agreement_on_the_Withdrawal_of_the_United_Kingdom_of_Great_Britain_and_Northern_Ireland_from_the_European_Union.pdf.

des Austrittsabkommens). Bei Zustimmung zum (bisherigen) Austrittsabkommen oder Verlängerung der Austrittsverhandlungen ändert sich in Bezug auf die Verarbeitung personenbezogener Daten daher vorerst nichts.

Bei einem Austritt wird das Vereinigte Königreich zu einem sogenannten Drittstaat. Sofern bis zu diesem Datum noch kein Angemessenheitsbeschluss der EU-Kommission im Sinne des Artikel 45 DSGVO vorliegt, muss jede verantwortliche Stelle, die personenbezogene Daten aus einem Mitgliedstaat der EU in das Vereinigte Königreich übermittelt, auf den Brexit vorbereitet sein, um die datenschutzrechtlichen Anforderungen auch nach dem Austritt sicherzustellen. Hierzu gehört die Schaffung geeigneter Garantien, wie beispielsweise der Verwendung der EU-Standardschutzklauseln.[45] Bei Vereinbarung von Binding Corporate Rules ist das Genehmigungsverfahren von Aufsichtsbehörden in zeitlicher Hinsicht besonders zu berücksichtigen.[46] Kommt es zum Austritt und haben die verantwortlichen Stellen bis dahin nicht für geeignete Garantien gesorgt, stellt jede Datenübermittlung in das Vereinigte Königreich einen sanktionsbehafteten Verstoß dar (Artikel 5 Abs. 1 lit. a, Artikel 44, Artikel 83 DSGVO). Ein solcher Verstoß kann durch eine Aufsichtsbehörde geahndet werden (siehe Befugnisse in Artikel 83 DSGVO). Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz weist etwa darauf hin, dass Aufsichtsbehörden die Datenübermittlung gemäß Artikel 58 Abs. 2 lit. j DSGVO aussetzen können und gemäß Artikel 83 Abs. 5 lit. c DSGVO eine zusätzliche Möglichkeit haben, eine Geldbuße zu verhängen, wenn es zu Verstößen gegen die Vorgaben für Datenübermittlungen in Drittländer kommt.[47] Er führt weiterhin aus, dass es aufgrund des hohen Datenschutzniveaus im Vereinigten Königreich zwar nicht sehr wahrscheinlich sei, dass von diesen Maßnahmen Gebrauch gemacht werden muss, aber dennoch möglich und damit für den Einzelfall nicht ausgeschlossen.[48]

Weiterhin müssen die verantwortlichen Stellen ebenso die internen Prozesse im Rahmen ihres Datenschutzmanagements überprüfen und ggf. anpassen. Hierzu gehört die Überarbeitung des Verzeichnisses für Verarbeitungstätigkeiten, insbesondere die Benennung der Datenübermittlungen in Drittländer (Artikel 30 DSGVO) und die Prüfung, inwieweit eine Datenschutz-Folgenabschätzung notwendig ist (Artikel 35 DSGVO). Auch müssen die Datenschutzhinweise angepasst werden, da über die Datenübermittlung in ein Drittland zu informieren ist (Artikel 13 Absatz 1 lit. f, Artikel14 Abs. 1 lit. f DSGVO) und bei einem Auskunftsersuchen der betroffenen Person sichergestellt werden muss, dass ebenso über die Datenübermittlung in ein Drittland beauskunftet wird (Artikel15 Abs. 1 lit. c, Abs. 2 DSGVO).

Der dafür notwendige Zeitaufwand ist von den verantwortlichen Stellen zu berücksichtigen.

[45] Siehe hierzu Fragen 1 bis 3.
[46] Siehe hierzu Frage 3.
[47] Siehe die Ausführungen des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz, abrufbar unter https://www.datenschutz.rlp.de/de/themenfelder-themen/brexit/.
[48] Siehe die Ausführungen des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz, abrufbar unter https://www.datenschutz.rlp.de/de/themenfelder-themen/brexit/.