

Mag. (FH) Christine Aschbacher
Bundesministerin

Herrn
Präsidenten des Nationalrates
Mag. Wolfgang Sobotka
Parlament
1017 Wien

christine.aschbacher@bmafj.gv.at
+43 1 711 00-0
Untere Donaustraße 13-15, 1020 Wien

Geschäftszahl: 2020-0.620.030

Ihr Zeichen: BKA - PDion (PDion)3569/J-NR/2020

Wien, am 25. November 2020

Sehr geehrter Herr Präsident,

die Abgeordneten zum Nationalrat Petra Oberrauner, Genossinnen und Genossen haben am 25.09.2020 unter der **Nr. 3569/J** an mich eine schriftliche parlamentarische Anfrage betreffend **Umsetzungsstand EuGH C-311/18** gerichtet.

Diese Anfrage beantworte ich nach den mir vorliegenden Informationen wie folgt:

Zu den Fragen 1 bis 7

- *Welche Schlussfolgerungen haben Sie aus dem Judikat EuGH C-311/18 für die unmittelbare Tätigkeit ihres Ministeriums bzw. nachgelagerter Dienststellen gezogen?*
- *Arbeiten Sie in Ihrem Ministerium oder in den - Ihrem Ministerium nachgelagerten - Dienststellen mit Software die möglicherweise Daten von Österreicherinnen und Österreichern rechtswidrig an ausländische Server außerhalb der EU schickt?*
Wenn ja, um welche Software handelt es sich und welche Maßnahmen haben Sie getroffen- bzw. planen Sie, um die betroffenen Menschen besser zu schützen?
- *Haben Sie Handlungsempfehlungen ausgearbeitet, damit ihr Ministerium und ihm nachgelagerte Dienststellen technisch in die Lage versetzt werden die persönlichen Daten von österreichischen Bürgerinnen und Bürgern zu schützen und auf Servern innerhalb der EU zu speichern? Wenn nein, warum nicht?*
- *Haben Sie Handlungsempfehlungen ausgearbeitet, wie ihr Ministerium und ihm nachgelagerte Dienststellen vorgehen müssen, wenn sie bislang Software eingesetzt*

haben, bei der technisch nicht ausschließbar ist, dass persönliche und sensible Daten von österreichischen Bürgerinnen und Bürgern auf Servern außerhalb der EU in Drittstaaten gespeichert oder verarbeitet werden? Wenn nein, warum nicht?

- *Haben Sie Handlungsempfehlungen ausgearbeitet, wie ihr Ministerium und ihm nachgelagerte Dienststellen vorgehen können, um Softwareumstellungen vorzunehmen, mit denen die Daten der österreichischen Bürgerinnen und Bürger auf Servern innerhalb der EU gespeichert oder verarbeitet werden, damit sie sich EU-Datenschutzrechts konform verhalten? Wenn nein, warum nicht?*
- *Haben Sie mit Ihren IT-Beratern im Ministerium das Problem der nicht rechtskonformen Verarbeitung von Daten durch die von ihrem Ministerium und ihm nachgelagerte Dienststellen eingesetzte Software erhoben, geprüft, analysiert und daraus Schlussfolgerungen hinsichtlich der rechtlichen Konsequenz und der verwendeten Software gezogen? Wenn ja, zu welchem Ergebnis sind sie gekommen? Wenn nein, warum nicht?*
- *Haben Sie mit Ihren Regierungskollegen, insbesondere der Bundesministerin für Digitalisierung und Wirtschaftsstandort oder der Bundesministerin für EU und Verfassung im Bundeskanzleramt eine Lösung für dieses Problem erarbeitet? Wenn nein, warum nicht?*

Einleitend darf ich festhalten, dass in meinem Ressort grundsätzlich keine Datenübermittlungen in Drittländer stattfinden. Die IT-Infrastruktur wird von der BRZ GmbH bereitgestellt und Datenverarbeitungen erfolgen somit in Österreich bzw. innerhalb der Europäischen Union. Auch bei sonstigen Auftragsverarbeitungen wird vertraglich dafür Sorge getragen, dass außerhalb des europäischen Raums keine Verarbeitungen erfolgen. Beim notwendigen passiven Einsatz von Videokonferenztools kann eine Datenübertragung in Länder mit nicht gleichwertigem Datenschutzniveau nicht ausgeschlossen werden. Zurzeit wird als Übergangslösung für Videokonferenzen, das im Bund weit verbreitete MS-Teams verwendet, bis eine einheitliche bundesweite Lösung (derzeitige Präferenz JITSI) implementiert wird.

Grundsätzlich werden Software und Systeme nur auf eigenen Servern und in der BRZ GmbH betrieben. Somit verbleiben personenbezogene Daten im eigenen Bereich.

Für den ausgegliederten Bereich darf ich Folgendes festhalten:

Das Arbeitsmarktservice (AMS) hat bereits vor dem angeführten Urteil des EuGHs seine IT-Strategie darauf ausgerichtet, die Systeme nach Möglichkeit in den Rechenzentren des bzw. der IT Outsourcing Partner IBM Österreich und BRZ GmbH zu betreiben. Bei beiden Partnern gibt es umfangreiche Auftragsverarbeitungsverträge bzw. bereits bei den Betriebsverträgen Vorgaben, dass die Daten der AMS Kundinnen und Kunden in Rechenzentren in Österreich verarbeitet und gespeichert werden. Eine eventuelle Verarbeitung im EU Raum bedarf der

expliziten Genehmigung durch das AMS. Hierbei ist eines der wesentlichen Kriterien die Einhaltung der DSGVO.

Das AMS setzt grundsätzlich keine Software oder Software „as a Service“ ein, die standardmäßig personenbezogene Daten außerhalb der EU speichert. Gegenwärtig werden im AMS für interne wie externe Zwecke „Cisco Webex“ als Online Meeting Tool sowie „GoToWebinar“ und „GoToTraining“ eingesetzt. Auch hierbei wurde auf grundsätzliche Vorgaben wie Verarbeitung innerhalb der EU und Einhaltung des DSGVO geachtet. Das AMS überprüft jährlich die bestehenden Verträge mit den IT-Dienstleistern bezüglich Einhaltung der erforderlichen rechtlichen Bestimmungen betreffend Informationssicherheit und Datenschutz. Bei Bedarf erfolgt eine entsprechende Anpassung.

Im Bereich der IEF-Service GmbH werden beim Einsatz von Software keine Daten von Österreicherinnen und Österreichern an außereuropäische Server übermittelt.

Bereits vor dem gegenständlichen Judikat wurden in der IEF-Service GmbH weitgehend österreichische bzw. europäische Softwarelösungen verwendet. Wo dies nicht möglich war, wurde durch die IEF-Service GmbH sichergestellt, dass Individualdaten nicht auf außereuropäischen Servern gespeichert werden. Die Datenübermittlung an Dritte erfolgt ausschließlich unter strikter Einhaltung der DSGVO. Die von der IEF-Service GmbH bis dato umgesetzte Vorgangsweise wurde durch das gegenständliche Urteil bestätigt und wird unter gleichzeitiger genauer Beobachtung der weiteren Softwareentwicklung im Rahmen der Beschaffungsplanung weiterverfolgt.

Weiters koordiniert das Bundeskanzleramt eine ressortübergreifende Datenschutz-Strategie zum Thema „Aufhebung des Privacy Shield und Cloud Computing – rechtskonforme Datenübertragung in die USA und sonstige Drittstaaten“. Es ist derzeit nicht absehbar, wann es Leitlinien oder neue Abkommen europäischer Gremien (EDSA, EK), Verhandlungserfolge mit den einschlägigen Anbietern, Zertifizierungen etc. geben wird. Die aktuelle, kurzfristige Zielsetzung besteht daher darin, eine von allen Ressorts nutzbare Fragenliste zu formulieren, die absichern soll, dass Anbieter von Clouddiensten DSGVO-konforme Garantien bieten. Derzeit wird auf wissenschaftlicher Basis diese Fragenliste erstellt. Diese wird dem Bundesministerium für Arbeit, Familie und Jugend zur Verfügung gestellt werden, um im Sinne der aktuellen Rechtsprechung des EuGH in der Rechtssache „Schrems II“ sicherstellen zu können, dass Cloud-Dienste (wie sie z.B. von Microsoft angeboten werden) auch datenschutzrechtskonform von der Republik eingekauft werden können, indem diese konkreten Fragen schon im Vorfeld gestellt und abgeklärt werden.

Zur Frage 8

- *Gibt es eine Empfehlung ihres Ministeriums zur Einsparung von IT-Kosten auf Cloudprodukte privater Anbieter bzw. bestimmter Unternehmen zu setzen? Wurde diese Empfehlung an die neue Rechtslage angepasst? Wenn nein, warum nicht?*

Wenn ja, mit welchem Inhalt (bitte um Beilage des aktuellen Textstandes zu Anfragebeantwortung)? Gibt es angesichts der aktuell geänderten Rechtslage Überlegungen im Ministerium den Einsparungskurs bei der IT-Soft- und Hardware zu überdenken?

Nachdem die BRZ GmbH für das Betreiben des IKT-Systems des Bundesministeriums für Arbeit, Familie und Jugend zuständig ist, können dahingehend umfassende Kostenempfehlungen und/oder Einsparungsempfehlungen nur seitens der BRZ GmbH abgegeben werden. Nachdem mein Ressort seit 29. Jänner 2020 besteht können aufgrund dieser geringen Zeitspanne noch keine verbindlichen Aussagen getroffen werden. Es gibt daher keine dahingehende Empfehlung.

Im Zuge der Sparsamkeit, Wirtschaftlichkeit und Zweckmäßigkeit wird bei der Planung in Zusammenarbeit mit der BRZ GmbH sowie IKT-Beschaffungen im Bundesministerium für Arbeit, Familie und Jugend stets ein hoher Maßstab zugunsten der Kostenverantwortlichkeit angelegt. Aufgrund eines ordnungsgemäßen Dienstbetriebes vor allem hinsichtlich der IKT-Sicherheit wird dringend von internationalen Cloudlösungen abgeraten und insbesondere einheitliche bundesweite Lösungen, unter Inkaufnahme etwaiger höherer Kosten zugunsten der IKT-Sicherheit, präferiert.

Mag. (FH) Christine Aschbacher

