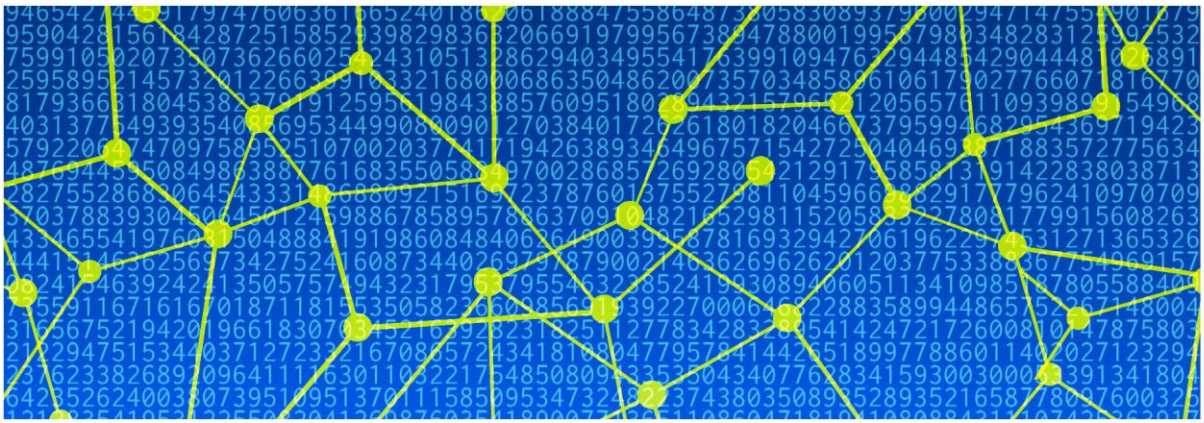

EUROPEAN DATA PROTECTION SUPERVISOR

Stellungnahme 5/2019

zur Überarbeitung der EU-Verordnungen über die Zustellung von Schriftstücken und die Beweisaufnahme in Zivil- und Handelssachen

EDPS

13. September 2019

Der Europäische Datenschutzbeauftragte (EDSB) ist eine unabhängige Einrichtung der EU und hat nach Artikel 52 Absatz 2 der Verordnung 2018/1725 im „Hinblick auf die Verarbeitung personenbezogener Daten [...] sicherzustellen, dass die Grundrechte und Grundfreiheiten natürlicher Personen, insbesondere ihr Recht auf Datenschutz, von den Organen und Einrichtungen der Union geachtet werden"; er ist gemäß Artikel 52 Absatz 3 „für die Beratung der Organe und Einrichtungen der Union und der betroffenen Personen in allen Fragen der Verarbeitung personenbezogener Daten" zuständig. Nach Artikel 57 Absatz 1 Buchstabe g der Verordnung (EU) 2018/1725 muss er „von sich aus oder auf Anfrage alle Organe und Einrichtungen der Union bei legislativen und administrativen Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten beraten".

Er wurde zusammen mit dem Stellvertretenden Datenschutzbeauftragten im Dezember 2014 ernannt und spezifisch mit einem konstruktiven und proaktiven Vorgehen beauftragt. In seiner im März 2015 veröffentlichten Fünf-Jahres-Strategie legt der EDSB dar, wie er diesen Auftrag auf verantwortungsvolle Weise zu erfüllen gedenkt.

Diese Stellungnahme enthält Empfehlungen zu zwei Vorschlägen der Kommission zur Überarbeitung der Verordnungen über die Zustellung von Schriftstücken und die Beweisaufnahme in Zivil- und Handelssachen, insbesondere im Hinblick auf die Nutzung eines IT-Systems für ihre Zwecke.

Zusammenfassung

Am 31. Mai 2018 legte die Europäische Kommission zwei Vorschläge vor; zum einen für eine Verordnung des Europäischen Parlaments und des Rates zur Änderung von Verordnung (EG) Nr. 1206/2001 des Rates vom 28. Mai 2001 über die Zusammenarbeit zwischen den Gerichten der Mitgliedstaaten auf dem Gebiet der Beweisaufnahme in Zivil- oder Handelssachen und zum anderen für eine Verordnung zur Änderung von Verordnung (EG) Nr. 1393/2007 des Europäischen Parlaments und des Rates über die Zustellung gerichtlicher und außergerichtlicher Schriftstücke in Zivil- oder Handelssachen in den Mitgliedstaaten. Die Vorschläge zielen hauptsächlich darauf ab, das reibungslose Funktionieren der justiziellen Zusammenarbeit in diesen Bereichen zu verbessern, indem unter anderem die Zustellung von Schriftstücken und die Beweisaufnahme über ein dezentrales IT-System vorgesehen sind.

Der EDSB ist der Auffassung, dass der Austausch personenbezogener Daten für die Schaffung eines Raums der Freiheit, der Sicherheit und des Rechts unerlässlich ist. Daher begrüßt er die allgemeinen Ziele der Vorschläge zur Verbesserung der Effizienz der justiziellen Zusammenarbeit in Zivil- oder Handelssachen in Bezug auf die Beweisaufnahme und die Zustellung von Schriftstücken, insbesondere durch Digitalisierung und den Einsatz von IT-Technologie. Er teilt die Auffassung, dass die vorgeschlagenen Verordnungen spürbare Auswirkungen auf das tägliche Leben der EU-Bürger haben könnten.

Diese Stellungnahme enthält drei wesentliche Empfehlungen, um den Gesetzgeber bei der Erreichung dieses sehr wichtigen Ziels konstruktiv zu unterstützen und gleichzeitig die Einhaltung der Charta und der DSGVO zu gewährleisten:

- Die Schaffung einer klaren Rechtsgrundlage für das IT-System, das für die Zustellung von Schriftstücken, Anträgen und Mitteilungen im Sinne dieser Verordnungen verwendet werden soll. Insbesondere für den Fall, dass das IT-System von einem Organ, einer Einrichtung, einer Agentur oder einem Amt der EU verwendet wird, sollte diese Rechtsgrundlage grundsätzlich in einem EU-Rechtsetzungsakt festgelegt werden. Auch für den Fall, dass die Verarbeitung personenbezogener Daten im Rahmen eines bereits vorhandenen IT-Systems erfolgen soll, empfiehlt der EDSB, die Verwendung eines solchen Systems im Rechtsetzungsakt selbst festzulegen. Das bereits vorhandene System, das zur Nutzung vorgesehen ist, sollte jedoch selbst ordnungsgemäß auf der Grundlage eines auf EU-Ebene erlassenen Rechtsakts eingerichtet werden, was bei e-CODEX derzeit nicht der Fall ist. Falls sich der EU-Gesetzgeber für die e-CODEX-Lösung entscheidet, sollte unverzüglich Abhilfe für das Fehlen eines Rechtsinstruments auf EU-Ebene zur Einrichtung und Regulierung des Systems geschaffen werden.

- Die Aufnahme einer allgemeinen Beschreibung der Merkmale des IT-Systems in die Rechtsetzungsakte selbst, beispielsweise der Verantwortlichkeiten im Bereich des Datenschutzes oder der einschlägigen geltenden Garantien. Die genauere Festlegung erfolgt in den Durchführungsrechtsakten. Insbesondere dann, wenn die Kommission oder ein anderes Organ, eine andere Einrichtung, eine andere Agentur oder ein anderes Amt der EU an der Nutzung des neuen Systems beteiligt wäre, sollten die Zuständigkeiten des (gemeinsam) für die Verarbeitung Verantwortlichen oder Auftragsverarbeiters im Idealfall im Rechtsakt festgelegt werden.

- Die Durchführung einer Folgenabschätzung zum Datenschutz bei der Ausarbeitung der Durchführungsrechtsakte.

Der EDSB gibt in dieser Stellungnahme weitere detaillierte Empfehlungen.

Der EDSB steht den Organen während des Gesetzgebungsverfahrens und während der Umsetzungsphase der Verordnungen nach deren Verabschiedung zur weiteren Konsultation zur Verfügung.

INHALTSVERZEICHNIS

DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 16,

gestützt auf die Charta der Grundrechte der Europäischen Union, insbesondere auf die Artikel 7 und 8,

gestützt auf die 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 (Datenschutz-Grundverordnung)[1],

gestützt auf die Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG[2], insbesondere Artikel 42 Absatz 1, Artikel 57 Absatz 1 Buchstabe g und Artikel 58 Absatz 3 Buchstabe c,

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

1. Einleitung und Hintergrund

1. Am 31. Mai 2018 hat die Kommission zwei Vorschläge[3] für eine Verordnung des Europäischen Parlaments und des Rates zur Änderung folgender Verordnungen angenommen:

   – Verordnung (EG) Nr. 1206/2001 des Rates vom 28. Mai 2001 über die Zusammenarbeit zwischen den Gerichten der Mitgliedstaaten auf dem Gebiet der **Beweisaufnahme in Zivil- oder Handelssachen** (nachstehend „Verordnung zur Beweisaufnahme“);

   – Verordnung (EG) Nr. 1393/2007 des Europäischen Parlaments und des Rates über die **Zustellung gerichtlicher und außergerichtlicher Schriftstücke in Zivil- oder Handelssachen in den Mitgliedstaaten** (nachstehend „Verordnung zur Zustellung von Schriftstücken“).

2. Die seit 2004 geltende Verordnung zur Beweisaufnahme sieht zwei Möglichkeiten der Beweisaufnahme zwischen den Mitgliedstaaten vor: die Beweisaufnahme durch das ersuchte Gericht und die unmittelbare Beweisaufnahme durch das ersuchende Gericht.

3. In der seit 2008 geltenden Verordnung zur Zustellung von Schriftstücken sind unterschiedliche Arten der Übermittlung von Schriftstücken von einem Mitgliedstaat in einen anderen vorgesehen. Sie können beispielsweise über Übermittlungs- oder Empfangsstellen oder durch Übermittlung auf konsularischem oder diplomatischem Weg zugestellt werden. Sie legt ferner einheitliche rechtliche Bedingungen für die unmittelbare grenzüberschreitende Zustellung von Schriftstücken per Post fest und sieht eine unmittelbare Zustellung durch die zuständige Person des betreffenden Mitgliedstaates vor, sofern dies nach dem Recht dieses Mitgliedstaates zulässig ist. Sie enthält gewisse Mindeststandards für den Schutz der Verteidigungsrechte. Die Anwendung der

Verordnung „*ist nicht auf Verfahren vor Zivilgerichten beschränkt, da ihr Anwendungsbereich auch „außergerichtliche" Schriftstücke umfasst, deren Zustellung in verschiedenen außergerichtlichen Verfahren (z. B. in Erbsachen vor einem Notar oder in Familiensachen vor einer Behörde) oder auch außerhalb eines Verfahrens notwendig sein kann*"[4].

4. Die Vorschläge sind im Arbeitsprogramm der Kommission für 2018 enthalten, und zwar unter REFIT-Initiativen – Ein auf gegenseitigem Vertrauen basierender Raum des Rechts und der Grundrechte[5]. Als Begleitdokument zu den Vorschlägen ist eine Folgenabschätzung beigefügt.[6]

5. Beide Vorschläge sehen die Übermittlung von Schriftstücken, Anträgen und Mitteilungen über ein verbindliches dezentrales IT-System vor, das aus nationalen IT-Systemen besteht, die durch eine Kommunikationsinfrastruktur miteinander verbunden sind und den sicheren und zuverlässigen grenzüberschreitenden Informationsaustausch zwischen den nationalen IT-Systemen ermöglichen. Ferner sehen sie die Anwendung von Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt vor[7].

6. Am 13. Februar 2019 verabschiedete das Europäische Parlament seine legislativen Entschließungen zu beiden Vorschlägen in erster Lesung[8], wobei es sich *unter anderem* auf die Einrichtung eines dezentralen IT-Systems einigte, sofern dieses System auf e-CODEX basiert und die Umsetzung eines solchen Systems durch delegierte Rechtsakte sichergestellt wird.

7. Am 6. Juni 2019 fand im Rat eine Orientierungsaussprache statt. Der Vorsitz kam zu dem Schluss, dass „*der Rat die Notwendigkeit einer Modernisierung unserer Prozesse im Bereich der justiziellen Zusammenarbeit in Zivil- und Handelssachen bekräftigt hat. Der Vorsitz stellte fest, dass ein dezentrales und gesichertes IT-System bevorzugt wird. Er fügte hinzu, dass die Minister die obligatorische Nutzung des Systems nur unter bestimmten Bedingungen akzeptieren könnten, einschließlich einer längeren Übergangsfrist und eines von der Kommission zur Verfügung zu stellenden Back-End-Referenzsystems. Eine Liste der notwendigen Ausnahmen ist ebenfalls zu berücksichtigen. Schließlich stellte der Vorsitz fest, dass e-CODEX die zu diesem Zweck zu verwendende Softwarelösung sein könnte. Auf technischer Ebene müssen weitere Arbeiten durchgeführt werden.*"[9]

8. Am 23. April 2019 hat die Kommission beim Europäischen Datenschutzbeauftragten (nachstehend „EDSB") einen Antrag auf Anhörung eingereicht, um die Konformität beider Vorschläge mit der Datenschutz-Grundverordnung (nachfolgend „DSGVO") zu bewerten. Der EDSB begrüßt die Anhörung seitens der Kommission.

2. Empfehlungen

2.1. Rechtsgrundlage

9. Der EDSB ist der Auffassung, dass der Austausch personenbezogener Daten für die Schaffung eines Raums der Freiheit, der Sicherheit und des Rechts unerlässlich ist. Daher begrüßt er die allgemeinen Ziele der Vorschläge zur Verbesserung der Effizienz der justiziellen Zusammenarbeit in Zivil- oder Handelssachen in Bezug auf die Beweisaufnahme und die Zustellung von Schriftstücken, insbesondere durch

Digitalisierung und den Einsatz von IT-Technologie. Er teilt die Auffassung, dass diese Rechtsvorschriften spürbare Auswirkungen auf das tägliche Leben der EU-Bürger haben könnten.

10. Der EDSB weist darauf hin, dass für die Einrichtung eines neuen IT-Systems zur Verarbeitung personenbezogener Daten sowie für dessen wesentliche Bestandteile eine Rechtsgrundlage erforderlich ist[10]. Er betont, dass insbesondere dann, **wenn ein solches IT-System von einem Organ, einer Einrichtung, einer Agentur oder einem Amt der EU verwendet wird, diese Rechtsgrundlage grundsätzlich in einem EU-Rechtsetzungsakt festgelegt werden sollte.**

11. Auch für den Fall, dass die Verarbeitung personenbezogener Daten im Rahmen eines bereits vorhandenen IT-Systems erfolgen sollte, **empfiehlt der EDSB, die Verwendung eines solchen Systems im Rechtsetzungsakt selbst festzulegen. Das vorhandene System, das zur Nutzung vorgesehen ist, sollte jedoch selbst ordnungsgemäß auf der Grundlage eines auf EU-Ebene erlassenen Rechtsakts eingerichtet werden, was bei e-CODEX derzeit nicht der Fall ist. Falls sich der EU-Gesetzgeber für die e-CODEX-Lösung entscheidet, sollte unverzüglich Abhilfe für das Fehlen eines Rechtsinstruments auf EU-Ebene zur Einrichtung und Regulierung des Systems geschaffen werden.**

2.2. Rechtsetzungsakte

12. **Der EDSB empfiehlt, in die Rechtsetzungsakte eine allgemeine Beschreibung der Merkmale des IT-Systems aufzunehmen und diese in den Durchführungsrechtsakten näher auszuführen.** Diese Elemente, die auf einer Bewertung der Risiken für die Grundrechte des Einzelnen beruhen, sollten zumindest die Verantwortlichkeiten im Bereich des Datenschutzes (d. h. die Rolle des für die Verarbeitung Verantwortlichen, des gemeinsam für die Verarbeitung Verantwortlichen, des Auftragsverarbeiters, soweit zutreffend) sowie die einschlägigen geltenden Garantien abdecken, einschließlich derjenigen, die die Sicherheit der verarbeiteten personenbezogenen Daten gewährleisten. Die Wahrung des Datenschutzes ist nicht nur eine rechtliche Verpflichtung, sondern es handelt sich dabei auch um einen Faktor, der wesentlich zum Erfolg der geplanten Systeme beiträgt, indem zum Beispiel die Qualität der ausgetauschten Daten sichergestellt wird.

2.2.1. Grundsätze des Datenschutzes durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

13. In der Begründung beider Vorschläge wird betont, dass folgende „*[e]xterne Faktoren wichtig für den Schutz personenbezogener Daten im Rahmen des vorgeschlagenen Pakets sind*: – *die seit Mai 2018 geltende Datenschutz-Grundverordnung (DSGVO), die das Bewusstsein und umgehende Maßnahmen für die Gewährleistung der Sicherheit und Integrität von Datenbanken sowie schnelle Reaktionen auf Verletzungen der Privatsphäre in der Justiz fördert; (...)* “[11]. Da die DSGVO für die Verarbeitung personenbezogener Daten zum Zwecke der justiziellen Zusammenarbeit in Zivil- oder Handelssachen in beiden Verordnungen gilt, empfiehlt der EDSB, ihre Grundsätze bereits bei der Einrichtung des IT-Systems anzuwenden, insbesondere die in Artikel 25 der DSGVO genannten **Grundsätze des Datenschutzes durch Technikgestaltung und datenschutzfreundliche Voreinstellungen**.

14. In diesem Zusammenhang **begrüßt der EDSB die Festlegung einer allgemeinen Systemarchitektur in den Rechtsetzungsakten selbst und die Verpflichtung zu einem zuverlässigen Informationsaustausch sowie die Notwendigkeit, Vertrauensdienste im Sinne der Verordnung (EU) Nr. 910/2014 des europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG zu verwenden**[12]. Er weist darauf hin, dass die Wahl der IT-Systemarchitektur zur Minimierung der Auswirkungen auf den Datenschutz auf der Grundlage einer Bewertung der Risiken für die Personen getroffen werden sollte, deren Daten verarbeitet werden, und nicht danach, welche Architektur die möglichen Verantwortlichkeiten der Mitgliedstaaten oder der Organe der EU minimiert. Generell könnte eine dezentrale Architektur in der Tat einzelne Fehlerquellen vermeiden und das Prinzip der Datenminimierung unterstützen, es sei denn, es besteht ein konkreter Bedarf an zentralen Funktionen.

15. In der Begründung beider Vorschläge wird betont, dass der weitere wichtige externe Faktor, der berücksichtigt werden muss, die „*anhaltenden Bedrohungen der Cybersicherheit im öffentlichen Sektor*“ sind. *„Es ist mit einer steigenden Zahl von Angriffen auf die öffentliche IT-Infrastruktur zu rechnen, die sich auch auf die Justiz in den Mitgliedstaaten auswirken. Ihre Folgen könnten sich durch die zunehmende Verflechtung der IT-Systeme (auf nationaler und auf EU-Ebene) noch verschärfen.“*[13] Es ist äußerst wichtig, dass die in diesem IT-System verarbeiteten Daten vor möglichen Angriffen und Sicherheitsvorfällen geschützt sind. Insbesondere im Hinblick **auf den Vorschlag zur Beweisaufnahme empfiehlt der EDSB, die erforderlichen geeigneten Garantien zur Gewährleistung der Sicherheit von Videokonferenzen genauer zu festzulegen**[14]**.** Diese Garantien sollen im Durchführungsrechtsakt näher ausgeführt werden (siehe Abschnitt 2.3. unten).

2.2.2. Bestimmung der Verantwortlichkeiten

16. Der EDSB betont, dass die Wahl einer dezentralen Architektur automatisch bedeutet, dass die Mitgliedstaaten für die Zivil- oder Handelsdatenbanken und die Verarbeitung personenbezogener Daten innerhalb dieser Datenbanken verantwortlich sind. Genauer gesagt liegt die Verantwortung für die Datenbanken bei den zuständigen Behörden der Mitgliedstaaten. Damit sind sie für den Inhalt der Datenbanken und für die Integrität der ausgetauschten Informationen verantwortlich. Es muss unbedingt sichergestellt werden, dass die Zuständigkeiten für die Einhaltung der Datenschutzbestimmungen klar definiert und zugewiesen sind.

17. Die Vorschläge zielen zwar auf die Schaffung einer allgemeinen Architektur für das geplante IT-System ab, legen aber weder die Governance noch die allgemeinen Aufgaben und Verantwortlichkeiten der Mitgliedstaaten und der Kommission (falls vorhanden) fest. Diese Aufgaben und Verantwortlichkeiten sind jedoch für die Bestimmung des für die Verarbeitung Verantwortlichen und der entsprechenden Pflichten nach dem geltenden Datenschutzgesetz von wesentlicher Bedeutung. Soweit die Kommission oder ein anderes Organ, eine andere Einrichtung, eine andere Agentur oder ein anderes Amt der EU an der Nutzung des neuen Systems beteiligt wäre, sollten die Zuständigkeiten des (gemeinsam) für die Verarbeitung Verantwortlichen oder Auftragsverarbeiters im Idealfall im Rechtsakt festgelegt werden. **Der EDSB empfiehlt daher nachdrücklich, die Governance und die allgemeinen Aufgaben und Verantwortlichkeiten der Mitgliedstaaten und der**

Kommission oder anderer Organe, Einrichtungen, Agenturen oder Ämter der EU (falls zutreffend) im Rechtsetzungsakt festzulegen. Sollte die Kommission oder ein anderes Organ, eine andere Einrichtung, eine andere Agentur oder ein anderes Amt der EU bei der Verarbeitung dieser Daten eine Rolle spielen, würde Verordnung Nr. 2018/1725 auf diese Verarbeitung Anwendung finden.

18. Gibt es gemeinsam für die Verarbeitung Verantwortliche, gelten die Verpflichtungen gemäß Artikel 26 der DSGVO bzw. Artikel 28 der Verordnung Nr. 2018/1725. **Das Verhältnis der gemeinsam für die Verarbeitung Verantwortlichen und der Inhalt der verbindlichen Vereinbarungen, die zwischen ihnen gelten, sollten in den Durchführungsrechtsakten festgelegt werden.**

2.3. Durchführungsrechtsakte

19. Der EDSB weist darauf hin, dass für die Einrichtung des dezentralen IT-Systems lediglich im Vorschlag zur Zustellung von Schriftstücken der Erlass eines Durchführungsrechtsakts vorgesehen ist[15]. **Er empfiehlt daher, in beiden Vorschlägen einen solchen Durchführungsrechtsakt vorzusehen.**

20. In solchen Durchführungsrechtsakten sollten wichtige Elemente des Systems genauer festgelegt werden. Außerdem sollten sie dazu beitragen, die Einhaltung der Datenschutzanforderungen sicherzustellen, indem die erforderlichen Garantien für das IT-System näher spezifiziert werden. Daher **empfiehlt der EDSB, in den Rechtsetzungsakten für den Durchführungsrechtsakt auch die neuen Bestimmungen für elektronische Zustellungen[16] und für die unmittelbare Beweisaufnahme per Videokonferenz vorzusehen[17].**

21. Da die den Vorschlägen beigefügten Folgenabschätzungen keine eingehende Analyse der Auswirkungen dieser Vorschläge auf den Datenschutz enthalten, **empfiehlt der EDSB der Kommission nachdrücklich, bei der Ausarbeitung der Durchführungsrechtsakte eine Folgenabschätzung durchzuführen.** Dies gilt unbeschadet der Verpflichtungen der für die Verarbeitung Verantwortlichen gemäß DSGVO und gegebenenfalls gemäß Verordnung Nr. 2018/1725, insbesondere dann eine Datenschutz-Folgenabschätzung gemäß Artikel 35 der DSGVO bzw. Artikel 39 der Verordnung Nr. 2018/1725 durchzuführen, wenn die Bedingungen erfüllt sind[18].

22. Aus der Begründung beider Vorschläge[19]schließt der EDSB außerdem, dass es möglich wäre, dass das zukünftige IT-System für beide Vorschläge dasselbe ist und dass der Zugriff auf bestimmte Nutzer beschränkt wird: im Vorschlag zur Beweisaufnahme wäre die Anzahl der Nutzer auf die von den Mitgliedstaaten bestimmten Gerichte[20], zentralen Behörden und zuständigen Behörden im Sinne der Verordnung beschränkt; im Vorschlag zur Zustellung von Schriftstücken wäre die Anzahl der Nutzer hingegen auf die Übermittlungs- oder Empfangsstellen[21] und die von den Mitgliedstaaten bestimmten zentralen Einrichtungen beschränkt. Der EDSB **empfiehlt, dass in den Durchführungsrechtsakten Garantien festgelegt werden, die nur einer begrenzten Anzahl von zugelassenen Nutzern den Zugriff gewähren.**

23. Abschließend würden mit den Vorschlägen ein neuer Artikel 23a für die Verordnung über die Zustellung von Schriftstücken und ein neuer Artikel 22a für Verordnung über die Beweisaufnahme eingeführt. Nach diesen stellen die Mitgliedstaaten der Kommission die

Daten und sonstige Nachweise zur Verfügung, die für das Monitoring-Programm erforderlich sind, das die Kommission spätestens zwei Jahre nach Geltungsbeginn der Verordnungen erstellen wird. Der EDSB geht davon aus, dass diese Monitoring-Programme die Erhebung statistischer Daten erfordern würden[22] und **empfiehlt, die zu erhebenden statistischen Daten so genau wie möglich in den Durchführungsrechtsakten festzulegen.**

3. Schlussfolgerungen

24. Der EDSB begrüßt die allgemeinen Ziele der Vorschläge zur Verbesserung der Effizienz der justiziellen Zusammenarbeit, insbesondere durch die Digitalisierung und den Einsatz von IT-Technologie in Bezug auf die Beweisaufnahme und die Zustellung von Schriftstücken in Zivil- oder Handelssachen. Daher sollen die Organe der EU mit dieser Stellungnahme konstruktiv und objektiv beraten werden.

25. Der EDSB begrüßt die Festlegung einer allgemeinen Systemarchitektur im Rechtsetzungsakt selbst und die Verpflichtung zu einem zuverlässigen Informationsaustausch sowie die Notwendigkeit, Vertrauensdienste im Sinne von Verordnung (EU) Nr. 910/2014 zu verwenden.

26. Der EDSB spricht drei wichtige Empfehlungen aus, um die Einhaltung der Charta und der DSGVO zu gewährleisten:

- Die Schaffung einer klaren Rechtsgrundlage für das IT-System, das für die Zustellung von Schriftstücken, Anträgen und Mitteilungen im Sinne dieser Verordnungen verwendet wird. Insbesondere für den Fall, dass das IT-System von einem Organ, einer Einrichtung, einer Agentur oder einem Amt der EU verwendet wird, sollte diese Rechtsgrundlage grundsätzlich in einem EU-Rechtsetzungsakt festgelegt werden. Auch für den Fall, dass die Verarbeitung personenbezogener Daten im Rahmen eines bereits vorhandenen IT-Systems erfolgen soll, empfiehlt der EDSB, die Verwendung eines solchen Systems im Rechtsetzungsakt selbst festzulegen. Das bereits vorhandene System, das zur Nutzung vorgesehen ist, sollte jedoch selbst ordnungsgemäß auf der Grundlage eines auf EU-Ebene erlassenen Rechtsakts eingerichtet werden, was bei e-CODEX derzeit nicht der Fall ist. Falls sich der EU-Gesetzgeber für die e-CODEX-Lösung entscheidet, sollte unverzüglich Abhilfe für das Fehlen eines Rechtsinstruments auf EU-Ebene zur Einrichtung und Regulierung des Systems geschaffen werden.

- In die Rechtsetzungsakte selbst wird eine allgemeine Beschreibung der Merkmale des IT-Systems aufgenommen, beispielsweise der Verantwortlichkeiten im Bereich des Datenschutzes oder der einschlägigen geltenden Garantien. Die genauere Festlegung erfolgt in den Durchführungsrechtsakten. Für den Fall, dass die Kommission oder ein anderes Organ, eine andere Einrichtung, eine andere Agentur oder ein anderes Amt der EU an der Nutzung des Systems beteiligt wäre, sollten die Zuständigkeiten des (gemeinsam) für die Verarbeitung Verantwortlichen oder Auftragsverarbeiters im Idealfall im Rechtsakt festgelegt werden.

- Die Durchführung einer Folgenabschätzung zum Datenschutz bei der Ausarbeitung der Durchführungsrechtsakte.

27. Der EDSB empfiehlt ferner,

– in beiden Rechtsetzungsakten einen Durchführungsrechtsakt vorzusehen, um das IT-System weiter zu präzisieren, so dass die neuen Bestimmungen zur elektronischen Zustellung und zur unmittelbaren Beweisaufnahme per Videokonferenz in den Durchführungsrechtsakten berücksichtigt werden und somit auch bei diesen Verarbeitungsvorgängen spezifische Garantien enthalten sind.

– für den Fall, dass gemeinsam für die Verarbeitung Verantwortliche vorhanden sind, das Verhältnis zwischen den gemeinsam für die Verarbeitung Verantwortlichen und den Inhalt der verbindlichen Vereinbarungen, die zwischen ihnen gelten, in den Durchführungsrechtsakten festzulegen.

– in den Durchführungsrechtsakten Garantien festzulegen, die einer begrenzten Anzahl von zugelassenen Nutzern den Zugriff gewähren.

– die zu erhebenden statistischen Angaben in den Durchführungsrechtsakten so genau wie möglich festzulegen.

28. Abschließend weist der EDSB darauf hin, dass er der Kommission, dem Rat und dem Europäischen Parlament in den weiteren Phasen dieses Prozesses zur Konsultation zur Verfügung steht. Die in dieser Stellungnahme abgegebenen Empfehlungen erfolgen unbeschadet etwaiger zusätzlicher Anmerkungen, die der EDSB unter Umständen bei weiteren Fragen machen könnte. Er weist darauf hin, dass die Kommission gemäß Artikel 42 Absatz 1 der Verordnung 2018/1725 verpflichtet ist, bei der Ausarbeitung von Durchführungsrechtsakten und delegierten Rechtsakten, die Auswirkungen auf den Schutz der Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten haben, den Europäischen Datenschutzbeauftragten zu konsultieren. Der EDSB geht daher davon aus, dass er diesbezüglich zu den Bestimmungen der Entwürfe für die Durchführungsrechtsakte oder delegierten Rechtsakte zu einem späteren Zeitpunkt konsultiert wird.

Brüssel, 13. September 2019

Wojciech Rafał WIEWIÓROWSKI

Hinweise

[1] ABl. L 119 vom 4.5.2016, S. 1.
[2] ABl. L 295 vom 21.11.2018, S. 39 (nachstehend „Verordnung Nr. 2018/1725“)
[3] Vorschlag COM (2018)378 final (nachstehend „Vorschlag zur Beweisaufnahme“) und Vorschlag COM (2018)379 final (nachstehend „Vorschlag zur Zustellung von Schriftstücken“).
[4] Begründung, Seite 2.
[5] Arbeitsprogramm der Kommission für 2018: Agenda für ein enger vereintes, stärkeres und demokratischeres Europa (COM(2017)650 final vom 24.10.2017), Anhang II, Punkte 10 und 11.
[6] Arbeitspapier der Kommissionsdienststellen SWD(2018)285 und SWD(2018)287.
[7] Begründung zum Vorschlag zur Beweisaufnahme, S. 3 und zum Vorschlag zur Zustellung von Schriftstücken, S. 4: „*[z]war sind die Mitgliedstaaten grundsätzlich nicht daran gehindert, ihre Kommunikation zu digitalisieren, die bisherigen Erfahrungen und Prognosen dessen, was ohne Maßnahmen auf EU-Ebene geschehen würde, zeigen jedoch, dass nur sehr langsam Fortschritte erzielt würden und dass, selbst wenn die Mitgliedstaaten tätig werden, die Interoperabilität ohne unionsrechtlichen Rahmen nicht sichergestellt werden kann. Das Ziel des Vorschlags kann von den Mitgliedstaaten selbst nicht ausreichend verwirklicht werden, sondern nur auf Unionsebene.*“
[8] P8_TA(2019)0103 und P8_TA(2019)0104.
[9] Ergebnisse der Ratstagung (9970/19), S. 7, vorläufige Fassung verfügbar unter: https://www.consilium.europa.eu/media/39709/st09970-en19.pdf
Nach dem Papier des Vorsitzes (9566/19), Abs. 8 und 13 „*wird e-CODEX in den Folgenabschätzungen der Kommission, die beiden Vorschlägen beigefügt sind, als das geeignetste und einzige ohne weiteres zur Verfügung stehende IT-System erachtet. Die Entwicklung eines anderen dezentralen Systems würde bedeuten, dass sich dabei wieder dieselben Herausforderungen stellen würden wie bereits bei der Entwicklung von e-CODEX.*“ „*Eine der bestehenden Lösungen ist e-CODEX, ein System, das mit finanzieller Unterstützung der EU von einem Konsortium von Mitgliedstaaten über einen Zeitraum von fast zehn Jahren entwickelt wurde. E-CODEX wird derzeit für folgende Zwecke genutzt: für das System zur Verknüpfung von Unternehmensregistern (Business Registers Interconnection System – BRIS); für die Vernetzung der nationalen Insolvenzregister; für das System für den digitalen Austausch von elektronischen Beweismitteln. Allerdings wird e-CODEX, soweit Anwendungsfälle auf der Grundlage der freiwilligen Zusammenarbeit betroffen sind, noch nicht von allen Mitgliedstaaten umgesetzt und verwendet. In diesem Zusammenhang könnte die Kommission bei den Beratungen auf Gruppenebene für diejenigen Mitgliedstaaten, in denen es derzeit keine IT-Systeme zur Unterstützung elektronischer Verfahren gibt, die Entwicklung einer Referenzlösung für die Implementierung eines Back-End-Systems auf nationaler Ebene in Betracht ziehen, sofern eine ausreichend starke und breite Unterstützung der Delegationen für eine obligatorische elektronische Kommunikation vorhanden ist. Alle Systeme müssten technisch interoperabel und mit den gleichen technischen Spezifikationen (Protokolle, Normen, XML-Schemata und Abläufe) kompatibel sein.*“
[10] Siehe Stellungnahme des EDSB zur Entscheidung der Kommission vom 12. Dezember 2007 über den Schutz personenbezogener Daten bei der Umsetzung des Binnenmarktinformationssystems (IMI) (2008/49/EG), ABl. 2008/C 270/01, Abs. 20-22: „*Aufgrund der Rechtsprechung zur EMRK sollte kein Zweifel über den rechtlichen Status von Bestimmungen bestehen, die die Grundrechte einschränken. Diese Bestimmungen müssen in einem Rechtsakt, gestützt auf den EG-Vertrag, niedergelegt sein, der vor Gericht geltend gemacht werden kann. Anderenfalls würde Rechtsunsicherheit für die betroffene Person entstehen, da sie sich nicht darauf verlassen kann, sich vor Gericht auf die Vorschriften berufen zu können.*
21. Die Frage der Rechtssicherheit ist sogar noch bedeutender, da im Rahmen des EG-Vertrags in erster Linie die nationalen Gerichte zu entscheiden haben werden, welchen Wert sie der IMI-Entscheidung beimessen. Dies könnte zu unterschiedlichen Ergebnissen in den einzelnen Mitgliedstaaten, ja sogar innerhalb ein und desselben Mitgliedstaates führen. Eine derartige Rechtsunsicherheit ist nicht hinzunehmen
22. Das Fehlen eines Rechtsmittels (bzw. der Gewissheit, über ein Rechtsmittel zu verfügen) würde auf jeden Fall Artikel 6 der EMRK, in dem das Recht auf ein faires Verfahren niedergelegt ist, und der Rechtsprechung zu diesem Artikel zuwiderlaufen. In diesem Fall würde die Gemeinschaft ihren Verpflichtungen nach Artikel 6 des Vertrags über die Europäische Union („VEU“) nicht nachkommen, dem zufolge die Union die Grundrechte, wie sie von der EMRK gewährleistet werden, achtet.
[11] Vorschlag zur Beweisaufnahme, S. 6 und Vorschlag zur Zustellung von Schriftstücken, S. 9 und 10.
[12] ABl. L 257 vom 28.8.2014, S. 73.
[13] Vorschlag zur Beweisaufnahme, S. 6 und Vorschlag zur Zustellung von Schriftstücken, S. 9 und 10.
[14] Im Falle der Nutzung öffentlich zugänglicher elektronischer Kommunikationsdienste gelten die Anforderungen der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung

personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), (ABl. L 201 vom 31.7.2002, S. 37).

[15] Siehe neuer Artikel 18a, eingeführt durch Artikel 1 Absatz 12 des Vorschlags zur Zustellung von Schriftstücken.

[16] Siehe neuer Artikel 15a, eingeführt durch Artikel 1 Absatz 10 des Vorschlags zur Zustellung von Schriftstücken.

[17] Siehe neuer Artikel 17a, eingeführt durch Artikel 1 Absatz 4 des Vorschlags zur Zustellung von Schriftstücken.

[18] Siehe auch Artikel-29-Datenschutzgruppe, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung personenbezogener Daten im Sinne der Verordnung 2016/679 WP 248 rev.01, Fußnote 21 „wahrscheinlich ein hohes Risiko mit sich bringt": „*Wird eine DSFA in der Phase der Ausarbeitung der Rechtsvorschriften durchgeführt, die eine Rechtsgrundlage für eine Verarbeitung personenbezogener Daten bilden, ist vermutlich vor Inkrafttreten eine Überprüfung erforderlich, da die erlassenen Rechtsvorschriften in Bezug auf Fragen der Privatsphäre und des Datenschutzes nicht unbedingt mit dem Vorschlag übereinstimmen müssen. Darüber hinaus ist es möglich, dass zum Zeitpunkt der Verabschiedung der Rechtsvorschriften nicht genügend technische Details über die tatsächliche Verarbeitung personenbezogener Daten verfügbar sind, selbst wenn diesen eine DSFA beigefügt war. In solchen Fällen kann es sich als notwendig erweisen, noch vor der eigentlichen Verarbeitung eine spezifische DSFA durchzuführen.*"
Siehe auch EDSB „Rechenschaftspflicht in der Praxis Teil I: Aufzeichnungen, Register und der richtige Zeitpunkt für Datenschutz-Folgenabschätzungen", S. 10: „[...] *selbst wenn bereits bei der Vorschlagserarbeitung für die Rechtsgrundlage eine DSFA nach den Normen der Verordnung durchgeführt wurde, ist es sehr wahrscheinlich, dass vor Inkrafttreten eine Überprüfung erforderlich ist. Der Grund dafür ist, dass die erlassene Rechtsgrundlage in Bezug auf die Auswirkungen auf die Privatsphäre und den Datenschutz nicht unbedingt mit dem Vorschlag übereinstimmen muss. Darüber hinaus entsprechen in der Regel noch nicht alle Entscheidungen bezüglich der Technikgestaltung, die sich auf die Privatsphäre und den Datenschutz auswirken, der Rechtsgrundlage. In der Praxis stellen solche DSFA im Gesetzgebungsverfahren allenfalls die erste Iteration des DSFA-Prozesses dar.*"

[19] In Bezug auf die vorgeschlagenen Digitalisierungsmaßnahmen und deren Auswirkungen auf die Grundrechte wird im Vorschlag zur Beweisaufnahme außerdem erläutert, dass „*das System, das für den elektronischen Austausch zwischen den benannten Gerichten eingeführt werden soll, eine absolut zuverlässige und sichere technische Lösung sein muss, die die Integrität und den Schutz der übermittelten Daten gewährleistet. Ein im Vorhinein festgelegter Kreis der Nutzer des Systems (nur Gerichte und andere Justizbehörden der Mitgliedstaaten), bietet eine zusätzliche Gewähr für den ordnungsgemäßen Umgang mit personenbezogenen Daten. Zudem muss das System über eine dezentrale Struktur verfügen, die die direkte Kommunikation zwischen den Endpunkten ermöglicht und damit das Risiko durch Minimierung der Zahl der Daten verarbeitenden Stellen verringert*" (S. 6. [Hervorhebung hinzugefügt]). In der Begründung des Vorschlags zur Zustellung von Schriftstücken wird betont, dass „*der vorgeschlagene Übergang zur elektronischen Kommunikation Auswirkungen auf den Schutz personenbezogener Daten haben dürfte (Artikel 8 der Charta). Die technische Einrichtung und den Betrieb der elektronischen Infrastruktur bestimmen und kontrollieren die Mitgliedstaaten selbst, auch wenn die Infrastruktur zum Teil auf EU-Ebene entwickelt und finanziert wird. Die Infrastruktur sollte dezentral aufgebaut sein. Die Anforderungen des Datenschutzes an die verschiedenen Verfahren würden daher ausschließlich auf nationaler Ebene gelten*" (S. 9. [Hervorhebung hinzugefügt]). Es wird weiter erklärt, dass ein solches System „*eine sichere elektronische Kommunikation und einen sicheren elektronischen Austausch von Schriftstücken zwischen den Nutzern des dezentralen IT-Systems gewährleisten und eine automatische Aufzeichnung aller Stufen des Verfahrensablaufs ermöglichen würde. Zudem würde das System über Sicherheitsmerkmale verfügen, die gewährleisten, dass es nur von ermächtigten Teilnehmern mit überprüfter Identität genutzt werden kann*" (S. 8).

[20] Siehe Artikel 2 Absatz 2, Artikel 3 und Artikel 22 der Verordnung zur Beweisaufnahme. Im Rahmen des Vorschlags zur Beweisaufnahme wird angeregt, den Ausdruck „Gericht" als „jede Justizbehörde in einem Mitgliedstaat, die für die Durchführung von Beweisaufnahmen nach dieser Verordnung zuständig ist" zu definieren (Einfügung eines 4. Absatzes zu Artikel 1 der Verordnung). Hiermit soll verdeutlicht werden, dass dies z. B. auch Notariate einschließt, sofern diese nach nationalem Recht befugt sind, Aufgaben im Zusammenhang mit der Beweisaufnahme wahrzunehmen (Begründung, S. 8).

[21] Gemäß Artikel 2 der Verordnung über die Zustellung von Schriftstücken bestehen diese Stellen aus Beamten, Behörden oder sonstigen Personen, die für die Übermittlung gerichtlicher und außergerichtlicher Schriftstücke zwecks Zustellung in anderen Mitgliedstaaten und für den Erhalt solcher Schriftstücke von anderen Mitgliedstaaten zuständig sind. Sie werden von den Mitgliedstaaten benannt. Die Informationen werden der Kommission übermittelt und im Amtsblatt der Europäischen Union veröffentlicht (siehe Artikel 23 der Verordnung und Artikel 1 Absatz 3 des Vorschlags zur Zustellung von Schriftstücken, in dem ein neuer Artikel 3a Absatz 1 eingeführt wird).

[22] Siehe Liste der Indikatoren in der Folgenabschätzung für die Beweisaufnahme, S. 40 und in der Folgenabschätzung für die Zustellung von Schriftstücken, S. 54.