EUROPEAN DATA PROTECTION SUPERVISOR

Stellungnahme 9/2017

Stellungnahme des EDSB zum Vorschlag für eine Verordnung über die Agentur für das Betriebsmanagement von IT-Großsystemen im Bereich Freiheit, Sicherheit und Recht (eu-LISA)

9. Oktober 2017

Der Europäische Datenschutzbeauftragte (EDSB) ist eine unabhängige Einrichtung der EU und hat nach Artikel 41 Absatz 2 der Verordnung (EG) Nr. 45/2001 „im Hinblick auf die Verarbeitung personenbezogener Daten (...) sicherzustellen, dass die Grundrechte und Grundfreiheiten natürlicher Personen, insbesondere ihr Recht auf Privatsphäre, von den Organen und Einrichtungen der Gemeinschaft geachtet werden"; er ist „für die Beratung der Organe und Einrichtungen der Gemeinschaft und der betroffenen Personen in allen die Verarbeitung personenbezogener Daten betreffenden Angelegenheiten" zuständig. Gemäß Artikel 28 Absatz 2 der Verordnung (EG) Nr. 45/2001 ist die Kommission zur Konsultation des EDSB verpflichtet, „wenn [sie] einen Vorschlag für Rechtsvorschriften bezüglich des Schutzes der Rechte und Freiheiten von Personen bei der Verarbeitung personenbezogener Daten annimmt".

Er wurde zusammen mit dem Stellvertretenden Datenschutzbeauftragten im Dezember 2014 ernannt und speziell 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.

In dieser Stellungnahme geht es um den Auftrag des EDSB, die EU-Organe bezüglich der Datenschutzauswirkungen ihrer Politiken zu beraten und eine verantwortliche Politikgestaltung zu fördern, im Einklang mit Maßnahme 9 der Strategie des EDSB: „Förderung einer verantwortungsvollen und fundierten politischen Entscheidungsfindung". Der EDSB ist der Auffassung, dass die Einhaltung der Datenschutzbestimmungen ein Schlüsselelement für ein erfolgreiches effektives Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts ist.

Zusammenfassung

Seit ihrer Gründung im Jahr 2011 wurde die Europäische Agentur für das Betriebsmanagement von IT-Großsystemen im Bereich Freiheit, Sicherheit und Recht („eu-LISA“) nach und nach mit dem Betriebsmanagement des Schengener Informationssystems, des Visa-Informationssystems und des Systems Eurodac betreut. Vier Jahre nach der Aufnahme des Betriebs von eu-LISA führte die Kommission eine Gesamtbewertung durch. Das Ergebnis war die Vorlage des Vorschlags für eine Verordnung über die Europäische Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts am 29. Juni 2017.

Gemäß diesem Vorschlag soll eu-LISA hauptsächlich mit folgenden Aufgaben betraut werden: i) Betriebsmanagement der vorhandenen und zukünftigen IT-Großsysteme im Bereich Freiheit, Sicherheit und Recht, ii) Entwicklung verschiedener Funktionen zur Sicherstellung der Interoperabilität dieser Systeme, iii) Durchführen von Forschungsaktivitäten und Pilotprojekten und iv) Entwickeln, Verwalten und Hosten eines gemeinsamen IT-Systems für eine Gruppe von Mitgliedsstaaten, die sich bei der Umsetzung technischer Aspekte der EU-Rechtsvorschriften in dezentralen Systemen im Raum der Freiheit, der Sicherheit und des Rechts auf freiwilliger Basis für eine zentralisierte Lösung entscheiden.

Der Vorschlag für eine Verordnung über eu-LISA ist Teil eines größeren Prozesses zur Stärkung der Verwaltung der Außengrenzen und der inneren Sicherheit in der Europäischen Union und soll das Reagieren auf konkrete Sicherheitsrisiken ermöglichen. In der Tat werden gegenwärtig verschiedene legislative Vorschläge zu IT-Großsystemen mit dem Europäischen Parlament und dem Rat verhandelt (Einreise-/Ausreisesystem, Eurodac, Europäisches Reiseinformations- und -genehmigungssystem, Schengener Informationssystem und das Europäische Strafregisterinformationssystem für Drittstaatsangehörige). Diese legislativen Vorschläge betrauen eu-LISA mit dem Betriebsmanagement der oben genannten IT-Großsysteme.

In seiner Funktion als Aufsichtsbehörde von eu-LISA empfiehlt der EDSB, dass der Vorschlag für eine Verordnung über eu-LISA von einer detaillierten Folgenabschätzung im Hinblick auf das Recht auf Schutz der Privatsphäre und das Recht auf Datenschutz flankiert wird, die in der Charta der Grundrechte der Europäischen Union verankert sind.

Der EDSB erinnert ebenso daran, dass es derzeit keinen rechtlichen Rahmen für die Interoperabilität von IT-Großsystemen in der EU gibt. Daher könnte eu-LISA die Umsetzungsmaßnahmen nur dann ausarbeiten, wenn ein solcher rechtlicher Rahmen verabschiedet würde.

Schließlich hat der EDSB Bedenken hinsichtlich der Möglichkeit, dass eu-LISA eine gemeinsame zentralisierte Lösung für IT-Großsysteme entwickeln und bereitstellen könnte, die grundsätzlich dezentral sind. Die Architektur jedes einzelnen EU-weiten IT-Großsystems wird in einer konkreten Rechtsgrundlage klar festgelegt und kann nicht durch eine Übertragungsvereinbarung zwischen eu-LISA und einer Gruppe von Mitgliedsstaaten geändert werden. Sämtliche Änderungen der Architektur eines Systems können nur durch eine Änderung der jeweiligen Rechtsgrundlage erfolgen, der eine Folgenabschätzung und Durchführbarkeitsstudien vorauszugehen haben.

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 Artikel 7 und 8,

gestützt auf die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr[1] und 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)[2],

gestützt auf die Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr[3], insbesondere auf Artikel 28 Absatz 2, Artikel 41 Absatz 2 und Artikel 46 Buchstabe d —

gestützt auf den Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden[4], und auf die Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates[5],

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

1 EINLEITUNG UND HINTERGRUND

1. Die Europäische Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts (nachstehend „eu-LISA“) wurde durch die Verordnung (EU) Nr. 1077/2011 des Europäischen Parlaments und des Rates vom 25. Oktober 2011 errichtet[6]. Die Verordnung betreut eu-LISA mit dem Betriebsmanagement auf zentraler Ebene des Schengener Informationssystems der zweiten Generation (nachstehend „SIS II“)[7] und des Visa-Informations-Systems (nachstehend „VIS“)[8]. Die Verordnung 1077/2011 wurde durch die Verordnung 603/2013 ergänzt[9], die eu-LISA zusätzlich mit dem Management von Eurodac beauftragt hat.

2. Im Jahr 2016, vier Jahre nach dem Start von eu-LISA, führte die Kommission eine Bewertung[10] dieser Agentur durch. Dabei wurde festgestellt, dass die Wirksamkeit und Effizienz von eu-LISA verbessert werden müssen. In diesem Zusammenhang legte die Kommission am 29. Juni 2017 einen Vorschlag für eine Verordnung über die Europäische Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der

Sicherheit und des Rechts [11] (nachstehend „Vorschlag für eine Verordnung über eu-LISA“) vor.

3. Daneben hat die Kommission seit 2016 umfassendere Überlegungen dazu angestellt, wie die Verwaltung und Nutzung der Daten sowohl für die Grenzkontrolle als auch zu Sicherheitszwecken wirksamer und effizienter gestaltet werden kann. Infolgedessen hat die Kommission eine Mitteilung über solidere und intelligentere Informationssysteme für das Grenzmanagement und mehr Sicherheit angenommen[12] sowie den Abschlussbericht der hochrangigen Expertengruppe für Informationssysteme und Interoperabilität[13] und den Siebten Fortschrittsbericht zu einer wirksamen und echten Sicherheitsunion[14] mit Vorschlägen zu neuen Aufgaben und somit zu einem neuen Mandat für eu-LISA.

4. Der EDSB wurde vor der Veröffentlichung des Vorschlags für eine Verordnung über eu-LISA informell konsultiert und machte gegenüber der Kommission informelle Anmerkungen, die nur teilweise berücksichtigt wurden.

5. Ziel des Vorschlags für eine Verordnung über eu-LISA ist es, das Mandat der Agentur folgendermaßen zu erweitern:
   - Ermöglichen des Betriebsmanagements der gegenwärtigen und zukünftigen IT-Großsysteme im Raum der Freiheit, der Sicherheit und des Rechts;
   - Sicherstellen der Datenqualität in allen IT-Großsystemen, die von eu-LISA verwaltet werden;
   - Konzipieren der notwendigen Maßnahmen, um die Interoperabilität der Systeme zu ermöglichen;
   - Durchführen von Forschungsaktivitäten für das Betriebsmanagement von IT-Großsystemen;
   - Durchführen von Pilotprojekten, Machbarkeitsstudien und Testmaßnahmen;
   - Unterstützen und Beraten von Mitgliedsstaaten und der Kommission im Hinblick auf die Verbindung der einzelstaatlichen Systeme mit dem Zentralsystem;
   - Entwickeln, Verwalten und Bereitstellen eines gemeinsamen IT-Systems für eine Gruppe von Mitgliedsstaaten, die sich bei der Umsetzung technischer Aspekte der EU-Rechtsvorschriften in dezentralen Systemen im Raum der Freiheit, der Sicherheit und des Rechts auf freiwilliger Basis für eine zentralisierte Lösung entscheiden.

6. Der EDSB wird sich zunächst auf die Hauptempfehlungen zu dem Vorschlag über eine Verordnung zu eu-LISA konzentrieren. Diese Empfehlungen beziehen sich auf die wichtigsten Probleme, die der EDSB festgestellt hat, und die in jedem Fall im Gesetzgebungsverfahren gelöst werden müssen. Die ergänzenden Empfehlungen beziehen sich auf Punkte, die einer Klärung, zusätzlicher Informationen oder geringfügiger Änderungen bedürfen. Durch diese Unterscheidung soll es dem Gesetzgeber erleichtert werden, den in dieser Stellungnahme aufgegriffenen Hauptproblemen Priorität einzuräumen.

2 HAUPTEMPFEHLUNGEN

2.1 Auswirkungen auf Grundrechte

7. Der Vorschlag für eine Verordnung über eu-LISA konzentriert das Betriebsmanagement aller EU-weiten IT-Großsysteme im Bereich Justiz und Inneres in einer einzigen Agentur.

Da diese Systeme hochsensible Informationen über Einzelpersonen enthalten, sind die Auswirkungen auf die Grundrechte vollumfänglich zu bewerten, einschließlich der in Artikel 7 und 8 der Charta der Grundrechte der Europäischen Union verankerten Rechte auf Schutz der Privatsphäre und Schutz personenbezogener Daten.[15] Tatsache ist, dass die Konzentration aller EU-weiten IT-Großsysteme die Risiken des Missbrauchs und der Sicherheitsverstöße deutlich erhöhen kann. Allerdings müssen diese Risiken mit einer umfassenderen und geeigneten Bewertung angegangen werden. In der Begründung wird lediglich erwähnt, dass die Auswirkungen des Vorschlags für eine Verordnung über eu-LISA auf die Grundrechte *„begrenzt [sind], da die [EU-]Agentur bewiesen hat, dass sie das Betriebsmanagement des SIS, des VIS und der Eurodac-Datenbank sowie neue Aufgaben effektiv übernehmen kann.“*. Der Vorschlag über eine Verordnung zu eu-LISA enthält keine weiteren Belege für das Vorstehende.

8. Außerdem scheint der Vorschlag für eine Verordnung über eu-LISA nicht von einer Folgenabschätzung flankiert zu werden. eu-LISA wird mit dem Betriebsmanagement des Europäischen Reiseinformations- und -genehmigungssystems[16], des Schengener Informationssystems[17] und Eurodac[18] betraut, wofür die derzeitigen legislativen Vorschläge auch keine Folgenabschätzungen vorzusehen scheinen. Der EDSB erinnert außerdem daran, dass es sich hierbei um eine wichtige Bedingung der Strategie der Kommission für bessere Rechtsetzung handelt[19] und um eine wesentliche Voraussetzung, wenn Grundrechte auf dem Spiel stehen.

9. Neben dem oben erwähnten erweiterten Betriebsmanagement stellt der EDSB fest, dass der Vorschlag für eine Verordnung über eu-LISA außerdem auf verschiedene laufende legislative Vorschläge zu IT-Großsystemen Bezug nimmt, die gegenwärtig mit dem Europäischen Parlament und dem Rat verhandelt werden, d. h. das Einreise-/Ausreisesystem[20], Eurodac[21], das Europäische Reiseinformations- und -genehmigungssystem[22], das Schengener Informationssystem[23] und das Europäische Strafregisterinformationssystem für Drittstaatsangehörige[24]. Der Vorschlag für eine Verordnung über eu-LISA nimmt nicht nur allgemein auf die zusätzlichen Aufgaben Bezug, mit denen eu-LISA eventuell betraut wird, sondern geht weiter ins Detail und spricht konkrete Bestimmungen laufender Vorschläge an (Artikel 15 Buchstaben ee bis pp) und siehe Änderungen dieser laufenden Vorschläge vor (Artikel 46 und 47). Der EDSB hebt hervor, dass ohne den endgültigen Wortlaut der Instrumente, auf die verwiesen wird, die Bewertung der Auswirkungen des Vorschlags für eine Verordnung über eu-LISA auf das Grundrecht auf Datenschutz nicht umfassend sein kann.

10. **Weiterhin empfiehlt der EDSB, eine detaillierte Analyse der Erforderlichkeit einer Konzentration des Betriebsmanagements aller EU-weiten IT-Großsysteme auf eine Agentur und der sich daraus ergebenden Auswirkungen auf die Grundrechte durchzuführen oder bereitzustellen. Dabei ist eine konsequente Studie oder ein sonstiger faktengestützter Ansatz zu verwenden und es ist der breitere rechtliche Zusammenhang zu berücksichtigen, einschließlich der laufenden legislativen Vorschläge zu IT-Großsystemen.**

2.2 Interoperabilität

11. Artikel 9 des Vorschlags für eine Verordnung über eu-LISA verleiht eu-LISA die Befugnis, die erforderlichen Maßnahmen zu ergreifen, um die Interoperabilität von IT-Großsystemen

zu ermöglichen. Dieser Artikel ist sehr vage formuliert, denn er stellt nicht klar, ob nur bereits vorhandene IT-Großsysteme oder auch zukünftige Systeme betroffen sind. Der EDSB stellt fest, dass es derzeit keinen rechtlichen Rahmen für die Interoperabilität von IT-Großsystemen in der EU gibt. Die Mitteilung der Kommission über solidere und intelligentere Informationssysteme für das Grenzmanagement und mehr Sicherheit[25] sowie der Abschlussbericht der hochrangigen Expertengruppe für Informationssysteme und Interoperabilität[26] zeigen mögliche künftige Schritte auf, denen weitere erforderliche Durchführbarkeitsstudien und eine konkrete Folgenabschätzung vorausgehen müssen. Da diese in großem Umfang in weitere Initiativen eingeflossen sind, können sie nicht als Rechtsgrundlage für die materielle Umsetzung von Maßnahmen durch eu-LISA verwendet werden.

12. In diesem Zusammenhang erinnert der EDSB außerdem an seine Erklärung[27] zu dem Konzept der Interoperabilität in den Bereichen Migration, Asyl und Sicherheit. Zwar befürwortet der EDSB Initiativen zur Entwicklung eines wirksamen und effizienten Informationsmanagements und erkennt die Notwendigkeit einer Verbesserung des Informationsaustausches an, er hebt jedoch hervor, dass in einem Bereich, in dem die Auswirkungen auf Grundrechte potenziell groß sein können, zunächst auf politischer Ebene die politischen Ziele genau festgelegt und auf allen Ebenen die Kernbedürfnisse analysiert werden müssen, um schließlich die geeignetsten technischen Lösungen zu bestimmen. Wie in dieser Erklärung erwähnt, ist der EDSB der Ansicht, dass Interoperabilität auch zu einer wesentlichen Veränderung der gegenwärtigen Architektur von IT-Großsystemen führen wird und daher die Auswirkungen einer solchen Entscheidung auf die Informationssicherheit weiter analysiert werden müssen. Bevor irgendwelche Änderungen vorgenommen werden, die die Sicherheit aller Systeme beeinträchtigen können, ist es notwendig, eine zusätzliche Analyse der Informationssicherheit durchzuführen. **Daher empfiehlt der EDSB, zu erwägen, die gegenwärtig im Vorschlag für eine Verordnung über eu-LISA vorhandenen Verweise auf die Interoperabilität zu streichen.**

2.3 Zentralisierung von dezentralen IT-Systemen

13. Gemäß Artikel 12 Absatz 2 des Vorschlags für eine Verordnung über eu-LISA kann eu-LISA von einer Gruppe von Mitgliedsstaaten damit beauftragt werden, ein gemeinsames IT-System für diese Gruppe von Mitgliedsstaaten zu entwickeln, zu betreiben, aufrecht zu erhalten und bereitzustellen und dabei auf eine zentralisierte Lösung zu setzen, die bei der Umsetzung von Pflichten, die sich aus den EU-Rechtsvorschriften zu dezentralen Großsystemen ergeben, Unterstützung leistet. Gemäß dieser Bestimmung könnte eine Gruppe von Mitgliedsstaaten auf freiwilliger Basis eine Vereinbarung mit eu-LISA schließen, um eine gemeinsame zentralisierte Lösung zum Betrieb eines spezifischen Systems zu schaffen, auch wenn die Rechtsgrundlage dieses Systems eine dezentrale Architektur vorsieht, die von jedem Mitgliedsstaat einzeln betrieben wird. Eine derartige Vereinbarung müsste vorher von der Kommission und vom Verwaltungsrat von eu-LISA genehmigt werden.

14. Der EDSB hebt hervor, dass der Betrieb jedes IT-Großsystems auf einer konkreten Rechtsgrundlage basiert, in der die Systemarchitektur klar festgelegt ist, einschließlich der Zentralisierung oder Dezentralisierung des Systems. Der EDSB erinnert weiterhin an die Hierarchie der Rechtsakte in der EU, die im Vertrag über die Arbeitsweise der Europäischen Union festgelegt ist. Demnach können wesentliche Änderungen,

insbesondere Änderungen der Architektur eines vorhandenen IT-Systems, die in dessen Rechtsgrundlage festgelegt ist, nicht durch eine Übertragungsvereinbarung und auch nicht durch delegierte Rechtsakte oder Durchführungsbestimmungen der Kommission vorgenommen werden.[28] Eine solche Änderung der Systemarchitektur kann nur durch eine Änderung der Rechtsgrundlage erfolgen, der die entsprechende Folgenabschätzung und Durchführbarkeitsstudien vorauszugehen haben, aus denen sich klar die Notwendigkeit und Verhältnismäßigkeit einer eventuellen Zentralisierung ergibt. Eine solche Vereinbarung kann auch Zweifel bezüglich ihrer Rechtssicherheit, Transparenz, ihrer Auswirkungen auf die Funktionsweise des gesamten Systems und auf mögliche Veränderungen der Aufgaben aufwerfen. Die Übertragungsvereinbarung sollte nicht zur Umgehung der demokratischen Kontrolle verwendet werden, die Teil des Rechtsetzungsprozesses ist. Somit kann aus rechtlicher Sicht **die Architektur des Systems nicht durch eine Übertragungsvereinbarung zwischen eu-LISA und einer Gruppe von Mitgliedsstaaten geändert werden.**

15. Außerdem qualifiziert die Tatsache allein, dass Mitgliedsstaaten und eu-LISA sich in einer Übertragungsvereinbarung auf bestimmte Dienstleistungen einigen, eine solche Vereinbarung nicht als gültige Rechtsgrundlage für eu-LISA-Verarbeitungsprozesse. **Der EDSB empfiehlt daher, Artikel 12 Absatz 2 des Vorschlags für eine Verordnung über eu-LISA zu streichen.**

16. Daneben nimmt die Begründung zum Vorschlag für eine Verordnung über eu-LISA[29] auf die von der hochrangigen Expertengruppe für Informationssysteme und Interoperabilität festgestellte Erforderlichkeit Bezug, eine Durchführbarkeitsstudie zu einer zentralen Routing-Komponente und der Zentralisierung von Fluggastdatensätzen (PNR-Daten) vorzunehmen. Es muss unterstrichen werden, dass die PNR-Richtlinie erst im Mai 2018 anwendbar wird und keine Durchführbarkeitsstudie zur Zentralisierung erfolgt ist. Es ist somit schwer nachzuvollziehen, warum der Gesetzgeber versuchen sollte, das System zu zentralisieren, noch bevor das PNR-System vollständig in Betrieb ist, und ohne einen klaren Beleg dafür, dass die derzeitige Systemarchitektur unangemessen wäre und geändert werden müsste. **Der EDSB ist der Auffassung, dass eine solche Änderung der Systemarchitektur erst nach der Änderung der PNR-Richtlinie möglich ist.**

3 WEITERE EMPFEHLUNGEN

3.1 Statistiken

17. Der EDSB begrüßt Artikel 8, der neue Pflichten zur Datenqualität einführt, die zu einer größeren Glaubwürdigkeit der IT-Großsysteme im Bereich Justiz und Inneres beitragen können. Der EDSB weist darauf hin, dass Artikel 8 auch die Einrichtung eines zentralen Speichers für Berichte und Statistiken vorsieht. In diesem Zusammenhang erinnert der EDSB an seine früheren Stellungnahmen zu EES[30], ETIAS[31] und SIS[32], in denen er nachdrücklich davor warnte, dass die vorgeschlagene Lösung zur Bereitstellung von Statistiken eu-LISA eine schwere Bürde auferlegen würde, da eu-LISA neben den gegenwärtigen Produktionsdaten im Zentralsystem noch einen zweiten Datenspeicher aufrechterhalten und angemessen absichern müsste. Das bedeutet auch zusätzliche Aufgaben für den EDSB, der diesen zweiten Speicher überwachen müsste. **Der EDSB würde eine Lösung bevorzugen, die keinen weiteren Zentralspeicher erfordert, sondern stattdessen von eu-LISA verlangt, Funktionalitäten zu entwickeln, die den Mitgliedstaaten, der Kommission, eu-LISA und bevollmächtigten Agenturen die**

Möglichkeit geben, die notwendigen Statistiken direkt aus den Zentralsystemen zu extrahieren.

3.2 Überwachung

18. Da die Hautaufgabe von eu-LISA im Betrieb von Informationssystemen besteht, ist es wichtig, die Nutzung und den Zugang der Bediensteten von eu-LISA – hauptsächlich Administratoren, die befugt sind, jedwede Änderung vorzunehmen – zu den von der Agentur verwalteten Systemen zu überwachen.

19. Obgleich die konkrete Rechtsgrundlage für jedes IT-Großsystem die Überwachung und Aufzeichnung von Informationsoperationen vorschreibt, so scheinen diese hauptsächlich auf die Operationen der Mitgliedsstaaten und nicht auf die von eu-LISA durchgeführten internen Operationen konzentriert zu sein. Daher **empfiehlt der EDSB, in den Vorschlag für eine Verordnung über eu-LISA konkrete Bestimmungen zur Überwachung aufzunehmen, um die Bedeutung der Selbstüberwachung durch eu-LISA hervorzuheben.**

3.3 Informationssicherheits-Risikomanagement

20. Der EDSB stellt fest, dass in Artikel 2 Buchstabe g, Artikel 7, Artikel 15 Buchstabe y und Artikel 21 Buchstabe r „Sicherheit" als Informationssicherheit zu verstehen ist. Eine hohe Informationssicherheit lässt sich jedoch nur durch eine Analyse der Risiken für die Informationssicherheit erreichen, denen ein Informationssystem ausgesetzt ist. Der EDSB möchte die Bedeutung hervorheben, die die Durchführung eines angemessenen Informationssicherheits-Risikomanagements gemäß Artikel 22 der Verordnung (EG) Nr. 45/2001 sowie gemäß den Leitlinien des EDSB hat[33]. In diesem Sinne **empfiehlt der EDSB, alle Verweise auf die Informationssicherheit oder Sicherheitspläne beispielsweise durch die Formulierungen „die Einführung eines geeigneten Verfahrens zum Informationssicherheits-Risikomanagement"[34] oder „die Einführung eines geeigneten Informationssicherheits-Managementsystems"[35] zu ersetzen.**

3.4 Rolle des EDSB

21. Der EDSB begrüßt, dass in den Vorschlag für eine Verordnung über eu-LISA in Artikel 10 Absatz 3 die Entwicklungen in der Forschung aufgenommen wurden sowie in Artikel 11 Absatz 1 auf die Entwicklung von Pilotprojekten und in Artikel 31 Absatz 2 auf den Evaluierungsbericht Bezug genommen wird. Allerdings schlägt der EDSB vor, den Wortlaut „soweit Fragen des Datenschutzes betroffen sind" leicht zu ändern in „wenn die Verarbeitung personenbezogener Daten betroffen ist", um so den Zuständigkeitsbereich des EDSB besser widerzuspiegeln.

22. Als Datenschutzbehörde, die mit der Überwachung von eu-LISA beauftragt ist, ist der EDSB berechtigt, alle Informationen zu erhalten, die für die Durchführung seiner Aufgaben relevant sind. Um es dem EDSB somit zu ermöglichen, seine Aufgaben effizient auszuführen, einschließlich der Aufgabe der Durchsetzung, **sollte der EDSB in die Liste der Empfänger der Vorabinformationen über Pilotprojekte (Artikel 11 Absatz 1) und jährlichen Tätigkeitsberichte (Artikel 15 Absatz 1 Buchstabe s) aufgenommen werden.**

4 SCHLUSSFOLGERUNG

23. Nach sorgfältiger Analyse des Vorschlags für eine Verordnung über eu-LISA spricht der EDSB die folgenden Empfehlungen aus:
    - Es sollte eine detaillierte Folgenabschätzung durchgeführt oder bereitgestellt werden, um die Auswirkungen des Vorschlags für eine Verordnung über eu-LISA auf die Grundrechte leichter bewerten zu können, insbesondere im Hinblick auf die Konzentration von IT-Großsystemen in einer einzigen Agentur, und unter Berücksichtigung des breiteren rechtlichen Zusammenhangs, einschließlich laufender legislativer Vorschläge zu IT-Großsystemen.
    - Die gegenwärtig im Vorschlag für eine Verordnung über eu-LISA vorhandenen Verweise auf die Interoperabilität sollten gestrichen werden.
    - Die Bestimmung, die eine Änderung der Systemarchitektur auf Grundlage einer Übertragungsvereinbarung zwischen eu-LISA und einer Gruppe von Mitgliedsstaaten ermöglicht, sollte gestrichen werden.

24. Neben den wichtigsten Bedenken, die vorstehend genannt wurden, betreffen die Empfehlungen des EDSB in der vorliegenden Stellungnahme folgende Aspekte des Vorschlags für eine Verordnung über eu-LISA:
    - vom System generierte Statistiken;
    - interne Überwachung;
    - Informationssicherheits-Risikomanagement;
    - Rolle des EDSB und des Datenschutzbeauftragten.

25. Der EDSB steht gerne für weitere Beratung zu dem Vorschlag für eine Verordnung über eu-LISA zur Verfügung, auch im Hinblick auf gemäß der vorgeschlagenen Verordnung angenommene delegierte Rechtsakte oder Durchführungsrechtsakte, die Auswirkungen auf die Verarbeitung personenbezogener Daten haben könnten.

Brüssel,

Giovanni BUTTARELLI

Europäischer Datenschutzbeauftragter

Endnoten

[1] ABl. L 281 vom 23.11.1995, S. 31.
[2] ABl. L 119 vom 4.5.2016, S. 1.
[3] ABl. L 8 vom 12.1.2001, S. 1.
[4] ABl. L 350 vom 30.12.2008, S. 60.
[5] ABl. L 119 vom 4.5.2016, S. 89.
[6] ABl. L 286 vom 1.11.2011, S. 1-17.
[7] Verordnung (EG) Nr. 1987/2006 des Europäischen Parlaments und des Rates vom 20. Dezember 2006 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II), (ABl. L 381 vom 28.12.2006, S. 4), und Beschluss 2007/533/JI des Rates vom 12. Juni 2007 über die Errichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II), ABl. L 205 vom 7.8.2007, S. 63.
[8] Verordnung (EG) Nr. 767/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über das Visa-Informationssystem (VIS) und den Datenaustausch zwischen den Mitgliedstaaten über Visa für einen kurzfristigen Aufenthalt (VIS-Verordnung) (ABl. L 218 vom 13.8.2008, S. 60-81).
[9] Verordnung (EU) Nr. 603/2013 des Europäischen Parlaments und des Rates vom 26. Juni 2013 über die Einrichtung von „Eurodac" für den Abgleich von Fingerabdruckdaten zum Zwecke der effektiven Anwendung der Verordnung (EU) Nr. 604/2013 zur Festlegung der Kriterien und Verfahren zur Bestimmung des Mitgliedstaats, der für die Prüfung eines von einem Drittstaatsangehörigen oder Staatenlosen in einem Mitgliedstaat gestellten Antrags auf internationalen Schutz zuständig ist und über der Gefahrenabwehr und Strafverfolgung dienende Anträge der Gefahrenabwehr- und Strafverfolgungsbehörden der Mitgliedstaaten und Europols auf den Abgleich mit Eurodac-Daten sowie zur Änderung der Verordnung (EU) Nr. 1077/2011 zur Errichtung einer Europäischen Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts (ABl. L 180 vom 29.6.2013, S. 1-30).
[10] Bericht der Kommission an das Europäische Parlament und den Rat über die Funktionsweise der Europäischen Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts (eu-LISA), KOM(2017) 346, 29.6.2017.
[11] Vorschlag für eine Verordnung über die Europäische Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts, zur Änderung der Verordnung (EG) Nr. 1987/2006 und des Beschlusses 2007/533/JI des Rates sowie zur Aufhebung der Verordnung (EU) Nr. 1077/2011 KOM(2017) 352 final 29.6.2017.
[12] KOM(2016) 205 final, 6.4.2016.
[13] http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1
[14] KOM(2017) 261 final, 16.5.2017.
[15] Artikel 7 und 8 der Charta der Grundrechte der Europäischen Union, ABl. C 326 vom 26.10.2012, S. 391–407.
[16] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über ein Europäisches Reiseinformations- und -genehmigungssystem (ETIAS) und zur Änderung der Verordnungen (EU) Nr. 515/2014, (EU) 2016/399, (EU) 2016/794 und (EU) 2016/1624, KOM(2016) 731 final.
[17] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rats über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems (SIS) im Bereich der Grenzkontrollen, zur Änderung der Verordnung (EU) Nr. 515/2014 und zur Aufhebung der Verordnung (EG) Nr. 1987/2006, KOM(2016) 882 final; Vorschlag für eine Verordnung des Europäischen Parlaments und des Rats über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems (SIS) im Bereich der polizeilichen Zusammenarbeit und der justiziellen Zusammenarbeit in Strafsachen, zur Änderung der Verordnung (EU) Nr. 515/2014 und zur Aufhebung der Verordnung (EG) Nr. 1986/2006, des Beschlusses 2007/533/JI des Rates und des Beschlusses 2010/261/EU der Kommission, KOM(2016) 883 final, und Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Nutzung des Schengener Informationssystems für die Rückkehr illegal aufhältiger Drittstaatsangehöriger KOM(2016) 881 final.
[18] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Einrichtung von „Eurodac" für den Abgleich von Fingerabdruckdaten zum Zwecke der effektiven Anwendung der [Verordnung (EU) Nr. 604/2013 zur Festlegung der Kriterien und Verfahren zur Bestimmung des Mitgliedstaats, der für die Prüfung eines von einem Drittstaatsangehörigen oder Staatenlosen in einem Mitgliedstaat gestellten Antrags auf internationalen Schutz zuständig ist], für die Feststellung der Identität illegal aufhältiger Drittstaatsangehöriger oder Staatenloser und über der Gefahrenabwehr und Strafverfolgung dienende Anträge der Gefahrenabwehr- und Strafverfolgungsbehörden der Mitgliedstaaten und Europols auf den Abgleich mit Eurodac-Daten (Neufassung).

[18] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über ein Europäisches Reiseinformations- und -genehmigungssystem (ETIAS) und zur Änderung der Verordnungen (EU) Nr. 515/2014, (EU) 2016/399, (EU) 2016/794 und (EU) 2016/1624, KOM(2016) 731 final.
[19] Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, Bessere Ergebnisse durch bessere Rechtsetzung – Eine Agenda der EU und interinstitutionelle Vereinbarung zwischen dem Europäischen Parlament, dem Rat der Europäischen Union und der Europäischen Kommission über bessere Rechtsetzung.
[20] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über ein Einreise-/Ausreisesystem (EES) zur Erfassung der Einreise- und Ausreisedaten sowie der Einreiseverweigerungsdaten von Drittstaatsangehörigen an den Außengrenzen der Mitgliedstaaten der Europäischen Union und zur Festlegung der Bedingungen für den Zugang zum EES zu Gefahrenabwehr- und Strafverfolgungszwecken und zur Änderung der Verordnung (EG) Nr. 767/2008 und der Verordnung (EU) Nr. 1077/2011, KOM(2016) 194 final.
[21] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Einrichtung von „Eurodac" für den Abgleich von Fingerabdruckdaten zum Zwecke der effektiven Anwendung der [Verordnung (EU) Nr. 604/2013 zur Festlegung der Kriterien und Verfahren zur Bestimmung des Mitgliedstaats, der für die Prüfung eines von einem Drittstaatsangehörigen oder Staatenlosen in einem Mitgliedstaat gestellten Antrags auf internationalen Schutz zuständig ist], für die Feststellung der Identität illegal aufhältiger Drittstaatsangehöriger oder Staatenloser und über der Gefahrenabwehr und Strafverfolgung dienende Anträge der Gefahrenabwehr- und Strafverfolgungsbehörden der Mitgliedstaaten und Europols auf den Abgleich mit Eurodac-Daten (Neufassung).
[22] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über ein Europäisches Reiseinformations- und -genehmigungssystem (ETIAS) und zur Änderung der Verordnungen (EU) Nr. 515/2014, (EU) 2016/399, (EU) 2016/794 und (EU) 2016/1624, KOM(2016) 731 final.
[23] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rats über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems (SIS) im Bereich der Grenzkontrollen, zur Änderung der Verordnung (EU) Nr. 515/2014 und zur Aufhebung der Verordnung (EG) Nr. 1987/2006, KOM(2016) 882 final; Vorschlag für eine Verordnung des Europäischen Parlaments und des Rats über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems (SIS) im Bereich der polizeilichen Zusammenarbeit und der justiziellen Zusammenarbeit in Strafsachen, zur Änderung der Verordnung (EU) Nr. 515/2014 und zur Aufhebung der Verordnung (EG) Nr. 1986/2006, des Beschlusses 2007/533/JI des Rates und des Beschlusses 2010/261/EU der Kommission, KOM(2016) 883 final, und Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Nutzung des Schengener Informationssystems für die Rückkehr illegal aufhältiger Drittstaatsangehöriger KOM(2016) 881 final.
[24] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Einrichtung eines zentralisierten Systems für die Ermittlung der Mitgliedstaaten, in denen Informationen zu Verurteilungen von Drittstaatsangehörigen und Staatenlosen (TCN) vorliegen, sowie zur Ergänzung und Unterstützung des Europäischen Strafregisterinformationssystems (ECRIS) und zur Änderung der Verordnung (EU) Nr. 1077/2011 (ECRIS-TCN), KOM(2017) 344 final.
[25] Mitteilung der Kommission vom 6. April 2016 an das Europäische Parlament und den Rat „Solidere und intelligentere Informationssysteme für das Grenzmanagement und mehr Sicherheit", KOM(2016) 205 final.
[26] Abschlussbericht der hochrangigen Expertengruppe für Informationssysteme und Interoperabilität vom Mai 2017.
[27] Erklärung des EDSB vom 15. Mai 2017 zum Konzept der Interoperabilität in den Bereichen Migration, Asyl und Sicherheit.
https://edps.europa.eu/sites/edp/files/publication/17-05-08_statement_on_interoperability_en.pdf.
[28] Artikel 288 bis 291 des Vertrags über die Arbeitsweise der Europäischen Union, ABl. C 326 vom 26.10.2012, S. 47–390.
[29] Seite 8.
[30] Stellungnahme des EDSB vom 21. September 2016 zum zweiten EU-Paket „Intelligente Grenzen", Punkt 70.
[31] Stellungnahme des EDSB vom 6. März 2017 zu dem Vorschlag für ein Europäisches Reiseinformations- und -genehmigungssystem, Punkt 108.
[32] Stellungnahme des EDSB vom 2. Mai 2017 zur neuen Rechtsgrundlage für das Schengener Informationssystem, Punkt 36.
[33] Leitlinien des EDSB vom 21. März 2016 zu Sicherheitsmaßnahmen für die Verarbeitung personenbezogener Daten – Artikel 22 der Verordnung (EG) Nr. 45/2001 (nur EN) abrufbar unter:
https://edps.europa.eu/sites/edp/files/publication/16-03-21_guidance_isrm_en.pdf.
[34] Definiert in den ISO-Leitlinien 73:2009: Das Informationssicherheits-Risikomanagement ist eine systematische Anwendung von Managementstrategien, -prozessen und -verfahren auf die Aktivitäten im Zusammenhang mit der Risikokommunikation und -konsultation, der Herstellung des Kontextes sowie der Identifikation, Analyse, Bewertung, Behandlung, Überwachung und Überprüfung der Risiken.

[35] Definiert in ISO/IEC 27000:2014: Ein ISMS besteht aus Politiken, Verfahren, Richtlinien und den damit in Verbindung stehenden Ressourcen und Aktivitäten, die ganzheitlich von einer Organisation mit dem Ziel gemanagt werden, ihre Informationen zu schützen.