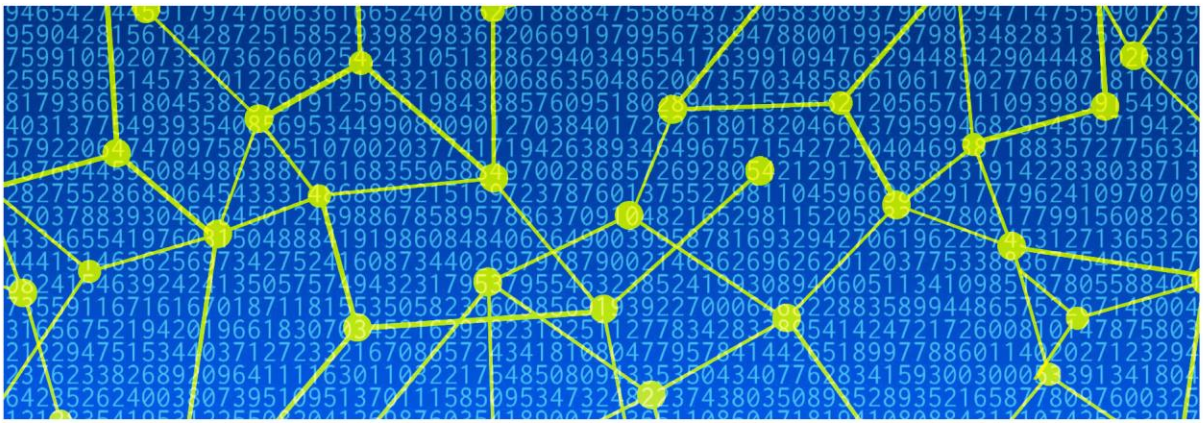

EUROPEAN DATA PROTECTION SUPERVISOR

Reflexionspapier zur Interoperabilität von Informationssystemen im Raum der Freiheit, der Sicherheit und des Rechts

17. November 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 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.

Das vorliegende Reflexionspapier soll einen Beitrag zu den Vorbereitungen des anstehenden Legislativvorschlags zur Interoperabilität von IT-Großsystemen der EU für Grenzmanagement und mehr Sicherheit leisten. Es ist vor dem Hintergrund des Auftrags des EDSB zu sehen, 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". Nach Auffassung des EDSB spielt die Einhaltung der Anforderungen des Datenschutzes eine Schlüsselrolle für ein wirksames und effizientes Informationsmanagement für Grenzmanagement und mehr Sicherheit.

Zusammenfassung

Grundsätzlich soll Interoperabilität zum Aufbau eines wirksamen und effizienten Informationsaustauschs beitragen und somit gewährleisten, dass zuständige Behörden auf nationaler und EU-Ebene die richtigen Informationen zum richtigen Zeitpunkt erhalten. Interoperabilität, sofern sie sorgfältig durchdacht umgesetzt wird, kann bestimmten Erfordernissen zuständiger Behörden, die IT-Großsysteme nutzen, gerecht werden und dabei helfen, die Gesamtkosten des Betriebs solcher Systeme zu senken. Interoperabilität kann auch im Interesse des Datenschutzes liegen. So kann beispielsweise die Verbindung von Informationssystemen, die eng miteinander verknüpften Zwecken dienen und zudem teilweise identische Daten enthalten, vermeiden helfen, dass die gleichen oder ähnliche Daten in den einzelnen Systemen vielfach gespeichert, validiert und auf den neuesten Stand gebracht werden.

Die terroristischen Anschläge im Hoheitsgebiet der EU haben Sicherheitsbedenken verstärkt. Darüber hinaus hat die EU in den letzten Jahren einen massiven Zustrom von Flüchtlingen und Migranten bewältigen müssen. Alle diese Ereignisse waren Anlass für die Europäische Kommission, mehrere Initiativen zu erwägen, darunter die Interoperabilität der IT-Großsysteme der EU, die für Migration, Grenzmanagement und/oder polizeiliche Zusammenarbeit aufgebaut wurden.

Einerseits halten wir fest, dass die Kommission möglicherweise Interoperabilität als Instrument für eine leichtere Nutzung von Systemen geplant hat, dass aber andererseits die Kommission möglicherweise erwägt, sie auf neue Möglichkeiten des Austauschs oder Abgleichs von Daten auszudehnen.

Da die Einführung von Interoperabilität vermutlich neue (oder geänderte) Formen der Verarbeitung personenbezogener Daten mit sich bringt, wäre für derartige Änderungen eine eindeutige Rechtsgrundlage unter voller Wahrung der EU-Charta der Grundrechte erforderlich. Neue oder geänderte Formen der Datenverarbeitung müssten insbesondere in dem einschlägigen Rechtsinstrument eindeutig definiert sein und gleichermaßen für ihre klar angegebenen Zwecke erforderlich sein und zu ihnen in einem angemessenen Verhältnis stehen.

Die Einhaltung der EU-Datenschutzvorschriften geht über die Grundsätze des Datenschutzes durch Technikgestaltung/datenschutzfreundliche Voreinstellungen, die Verpflichtung zur Anwendung von Sicherheitsmaßnahmen usw. hinaus und verlangt, dass zunächst einmal die Notwendigkeit und Verhältnismäßigkeit der Verarbeitung festgestellt wird.

Wir erwarten daher mit Spannung den anstehenden Legislativvorschlag der Europäischen Kommission, in dem die Probleme, die mit Interoperabilität gelöst werden sollen, klar umrissen werden sollten. Ferner sollte dort eindeutig festgelegt sein, für welche konkreten Zwecke welche Kategorien personenbezogener Daten im Rahmen ihrer künftigen Initiativen für Interoperabilität verarbeitet werden sollen. Damit wäre auch eine geordnete Debatte über Interoperabilität aus der Grundrechtsperspektive möglich. Sobald nähere Einzelheiten über die geplante Initiative bekannt sind, ist eine vollständige Bewertung der Auswirkungen der Interoperabilität auf die Grundrechte auf Privatsphäre und Datenschutz unbedingt geboten. Der anstehende Legislativvorschlag könnte in diesem Sinne eine Chance für die Gestaltung eines kohärenteren und schlüssigeren Rahmens bieten, die nicht ungenutzt verstreichen sollte.

INHALT

1 Laufende Initiativen im Bereich der „Interoperabilität“ von IT-Großsystemen

1 Die terroristischen Anschläge im Hoheitsgebiet der EU haben Sicherheitsbedenken verstärkt. Darüber hinaus hat die EU in den letzten Jahren einen massiven Zustrom von Flüchtlingen und Migranten bewältigen müssen. Diese Ereignisse waren Anlass für die EU-Kommission, mehrere Initiativen zu erwägen, darunter die Schaffung neuer IT-Großsysteme der EU[1], den Umbau bestehender Systeme[2] sowie die Interoperabilität all dieser Systeme.

2 In ihrer Mitteilung vom 6. April 2016 „*Solidere und intelligentere Informationssysteme für das Grenzmanagement und mehr Sicherheit*“ („Mitteilung von 2016“)[3] unterstrich die Kommission die Notwendigkeit einer besseren Interoperabilität von Informationssystemen; ferner legte sie ihre Ideen dazu dar, wie in Zukunft Informationssysteme entwickelt werden können. Die Kommission setzte eine hochrangige Sachverständigengruppe „Informationssysteme und Interoperabilität“ („HLEG“) ein. Die HLEG sollte sich mit den „rechtlichen, technischen und operativen Aspekten der verschiedenen Optionen für die Herstellung der Interoperabilität von Informationssystemen befassen und insbesondere die Notwendigkeit, die technische Durchführbarkeit und die Angemessenheit der verfügbaren Optionen und ihre Auswirkungen auf den Datenschutz prüfen“.[4]

3 Die HLEG legte Empfehlungen für die Stärkung und den Ausbau der EU-Informationssysteme und zur Interoperabilität zunächst in ihrem Zwischenbericht vom Dezember 2016[5] und später in ihrem Abschlussbericht vom Mai 2017[6] vor. Der EDSB war zur Teilnahme an den Arbeiten der HLEG eingeladen. Er gab eine Erklärung zum Konzept der Interoperabilität im Bereich Migration, Asyl und Sicherheit ab, die in den Abschlussbericht der HLEG aufgenommen wurde.

4 In ihrer Mitteilung „Auf dem Weg zu einer wirksamen und echten Sicherheitsunion - Siebter Fortschrittsbericht“[7] legt die Kommission einen neuen Ansatz für das Datenmanagement im Bereich Grenzen und Sicherheit in Anlehnung an die Mitteilung von 2016 und die Empfehlungen der HLEG dar. Diesem Ansatz zufolge sollten alle zentralisierten Informationssysteme der EU für Sicherheit, Grenzmanagement und Migrationssteuerung interoperabel sein, damit

- die Systeme mithilfe eines europäischen Suchportals gleichzeitig abgefragt werden können, wobei gegebenenfalls straffere Regeln für den Zugang der Strafverfolgungsbehörden festgelegt werden;
- die Informationssysteme einen gemeinsamen Dienst für den Abgleich biometrischer Daten nutzen, der die gleichzeitige Abfrage verschiedener Informationssysteme, in denen biometrische Daten erfasst sind, ermöglicht, gegebenenfalls mit der Kennzeichnung „Treffer“ oder „kein Treffer“, der sich entnehmen lässt, ob ein Zusammenhang mit entsprechenden biometrischen Daten in einem anderen System besteht;
- die Systeme auf einen gemeinsamen Speicher für Identitätsdaten, in dem alphanumerische Identitätsdaten erfasst sind, zurückgreifen, um zu ermitteln, ob eine Person in verschiedenen Datenbanken unter mehreren Identitäten registriert ist.

5 Am 8. Juni 2017 begrüßte der Rat die Haltung der Kommission und ihren Vorschlag für das weitere Vorgehen für das Erreichen der Interoperabilität von Informationssystemen bis 2020. Er forderte die Kommission auf, die Arbeit an drei Dimensionen der Interoperabilität fortzusetzen (nämlich dem europäischen Suchportal, dem Dienst für den Abgleich biometrischer Daten und einem gemeinsamen Speicher für Identitätsdaten).[8]

Am 27. Juli 2017 leitete die Kommission eine öffentliche Konsultation zur Interoperabilität der EU-Informationssysteme im Bereich Grenzen und Sicherheit ein[9]. Als Begleitdokument zur Konsultation lag eine erste Folgenabschätzung vor. In ihrer vorläufigen Planung vom 2. Oktober[10] nennt die Kommission das Datum 12. Dezember für die Annahme des Legislativvorschlags über Interoperabilität.

6 In Erwartung des anstehenden Legislativvorschlags stellt dieses Reflexionspapier einen weiteren Beitrag unsererseits dar. Später wird es noch eine offizielle Stellungnahme des EDSB gemäß Artikel 28 Absatz 2 der Verordnung (EG) Nr. 45/2001 geben.

2 Das Konzept der Interoperabilität

7 Unter Interoperabilität versteht man im Allgemeinen die Fähigkeit verschiedener Informationssysteme zur Kommunikation, zum Austausch von Daten und zur Nutzung der ausgetauschten Informationen. Interoperabilität gilt zwar häufig als rein technisches Konzept, doch sind wir der Auffassung, dass es im vorliegenden Kontext nicht von den Fragen getrennt werden kann, ob der Datenaustausch erforderlich, politisch wünschenswert oder rechtlich möglich ist. Oder anders gesagt: Auch wenn die Interoperabilität der Informationssysteme letztendlich mit technischen Mitteln hergestellt wird, müssen doch ihre Zwecke und ihr künftiger Geltungsbereich Gegenstand einer politischen Debatte sein.

8 Wir beobachten immer wieder, dass die technische Machbarkeit eines Datenaustauschs zwangsläufig dazu führt, dass diese Daten tatsächlich ausgetauscht werden. Man kann getrost davon ausgehen, dass technische Mittel auch genutzt werden, wenn sie einmal zur Verfügung stehen, oder in anderen Worten: Es besteht die Gefahr, dass in einem solchen Fall die Mittel das Ziel heiligen. Damit eine geordnete Debatte über die Risiken und Vorteile der Interoperabilität geführt werden kann, muss der Begriff unbedingt eine eindeutige und klare Bedeutung erhalten.

9 Wir halten fest, dass Interoperabilität auf verschiedenen Ebenen gegeben sein kann; sie kann von einer reinen Kommunikationsinfrastruktur zwischen zwei Systemen bis hin zur Fähigkeit dieser Systeme reichen, sowohl Informationen auszutauschen als auch die ausgetauschten Informationen zu verwenden. Wir räumen ein, dass Interoperabilität, sofern sie sorgfältig durchdacht umgesetzt wird, bei der Abdeckung bestimmten Erfordernissen zuständiger Behörden, die IT-Großsysteme nutzen, gerecht werden sowie dabei helfen kann, die Gesamtkosten des Betriebs solcher Systeme zu senken. Interoperabilität kann aber auch Vorteile im Hinblick auf den Datenschutz bieten. So kann beispielsweise die Verbindung von Informationssystemen, die eng miteinander verknüpften Zwecken dienen und zudem teilweise identische Daten enthalten, vermeiden helfen, dass die gleichen Daten in den einzelnen Systemen mehrfach gespeichert werden.[11]

10 Interoperabilität würde grundsätzlich darauf abheben, derzeit geltende Vorschriften effektiver und effizienter zu machen. Das von der Kommission geplante europäische Suchportal beispielsweise würde zuständige Behörden in die Lage versetzen, mehrere Systeme gleichzeitig anstatt jedes System für sich abzufragen. Werden solche Abfragen von befugten zuständigen Behörden unter voller Wahrung ihrer Zugriffsrechte und im Einklang mit den in den Rechtsgrundlagen niedergelegten jeweiligen Zwecken der einzelnen Systeme vorgenommen, bestünden aus Sicht des Datenschutzes keine grundlegenden Bedenken. Nutzer bekämen nur zu den Informationen Zugang, auf die sie zugreifen dürfen, und dies ausschließlich für den/die spezifischen Zweck(e) des betreffenden Systems.

11 Wir halten jedoch fest, dass die Kommission einerseits möglicherweise Interoperabilität als Instrument für eine leichtere Nutzung von Systemen geplant hat, dass aber die Kommission andererseits möglicherweise daran denkt, sie auf neue Möglichkeiten des Austauschs oder Abgleichs von Daten auszudehnen. So ist in der ersten Folgenabschätzung beispielsweise die Rede vom Einsatz eines gemeinsamen Dienstes für den Abgleich biometrischer Daten („BMS“), der den Abgleich biometrischer Daten über verschiedene Systeme hinweg ermöglichen soll. Ähnlich würden in einem „gemeinsamen Speicher für Identitätsdaten“ alphanumerische Daten (wie Namen und Geburtsdaten) zusammenkommen, die in den verschiedenen Systemen für Grenzmanagement und Sicherheit gespeichert sind. Der gemeinsame Einsatz von BMS und gemeinsamem Speicher für Identitätsdaten würde nun eine Identifizierung unter Verwendung alphanumerischer und/oder biometrischer Daten ermöglichen, um zu ermitteln, ob jemand mit mehreren Identitäten auftritt. Interoperabilität hat also neue Formen der Datenverarbeitung zur Folge, die durch die bestehenden Rechtsgrundlagen nicht abgedeckt sind und deren Auswirkungen auf die Grundrechte auf Privatsphäre und Datenschutz sorgfältig untersucht werden müssten.

3 Interoperabilität aus dem Blickwinkel des Datenschutzes

3.1 Personenbezogene Daten „müssen nach Treu und Glauben für festgelegte Zwecke verarbeitet werden“

12 Unserer Auffassung nach sollte Interoperabilität kein Selbstzweck sein, sondern stets einem Ziel dienen, das wirklich im öffentlichen Interesse liegt. In der ersten Folgenabschätzung ist die Rede von dem allgemeinen Ziel der „Entwicklung stärkerer und intelligenterer Informationssysteme für Grenzen und Sicherheit“. Im Anschluss daran werden die folgenden spezifischen Ziele genannt:

- sicherstellen, dass Endnutzer, insbesondere Grenzschutzbeamte, Beamte von Strafverfolgungsbehörden, Einwanderungsbeamte und Justizbehörden schnell und reibungslos Zugriff auf alle Informationen haben, die sie für die Wahrnehmung ihrer Aufgaben benötigen;
- den Zugriff für Strafverfolgungsbehörden auf Informationssysteme außerhalb des Bereichs Strafverfolgung erleichtern und straffen, sofern er für die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten erforderlich ist;
- eine Lösung für die Aufdeckung und Bekämpfung von Identitätsbetrug bereitstellen.[12]

13 Es sei in diesem Zusammenhang darauf hingewiesen, dass allgemeine politische Ziele wie die in der ersten Folgenabschätzung aufgeführten nicht unbedingt einem Ziel in

öffentlichem Interesse im Sinne des Gesetzes gleichzusetzen sind, beispielsweise im Sinne von Artikel 52 Absatz 1 der Charta, und auch nicht den Zielen der Datenverarbeitung nach dem Datenschutzrecht entsprechen. Bei den erwähnten Zielen scheint im Mittelpunkt zu stehen, was Interoperabilität im technischen Sinne erreichen würde. Nähere Erläuterungen zur geplanten Datenverarbeitung, dem öffentlichen Interesse und ihrem/ihren spezifischen Zweck(en) gibt es dort nicht. Statt dessen scheint die erste Folgenabschätzung die *Verarbeitung*, die eine Interoperabilität erleichtern oder ermöglichen würde (z. B. Konsultation, Zugriff, Verwendung, Abrufen usw. der Daten) mit den *Zwecken* der Verarbeitung gleichzusetzen.

14 Wir fordern die Kommission auf, die spezifischen Zwecke der geplanten Datenverarbeitung ganz klar zu beschreiben. Ziele wie „einen schnellen und reibungslosen Zugang zu Datenbanken gewährleisten“ können politisch sinnvoll sein. Für die Zwecke des Datenschutzrechts sind sie jedoch nicht spezifisch genug, da sie nicht mit der konkreten Verarbeitung genau definierter Kategorien personenbezogener Daten verknüpft sind. Folglich geben sie betroffenen Personen keine Auskunft darüber, welche ihrer personenbezogenen Daten für genau welche Zwecke verarbeitet werden und welches die Konsequenzen einer solchen Verarbeitung sind.

15 Es muss klar sein, dass die genaue Angabe des Zwecks unabdingbare Voraussetzung für die Anwendung vieler weiterer Grundsätze des Datenschutzes ist. Nur wenn klare und spezifische Zwecke angegeben werden, kann festgelegt werden, welche Daten erhoben werden, welche Aufbewahrungsfristen gelten, und wie mit allen anderen zentralen Aspekten der Verarbeitung personenbezogener Daten für den/die gewählten Zweck(e) umzugehen ist. Die Beschreibung des Ziels im öffentlichen Interesse entspricht möglicherweise nicht dem Erfordernis der Zweckspezifizierung, vor allem dann, wenn das öffentliche Interesse vielleicht mehrere Aspekte aufweist.[13] Wir empfehlen daher, im anstehenden Legislativvorschlag klar die Zwecke der verschiedenen geplanten Datenverarbeitungen festzulegen.

3.2 Klärung des Bedarfs an Interoperabilität

16 Eine klare Beschreibung der Zwecke der vorgeschlagenen Datenverarbeitung spielt auch eine zentrale Rolle bei der Beurteilung ihrer Notwendigkeit und Verhältnismäßigkeit. Diese Zwecke müssen hinreichend detailliert dargestellt werden, nicht nur, damit eine objektive Beantwortung Frage möglich ist, ob die vorgeschlagene Erhebung und Verwendung gesetzeskonform ist, sondern auch, um festzulegen, welche Garantien gelten sollten. Wir verweisen auf das „Toolkit zur Beurteilung der Erforderlichkeit von Maßnahmen“, das dem EU-Gesetzgeber leicht verständlich näherbringt, wie die Einhaltung von Artikel 7 und 8 sowie Artikel 52 Absatz 1 der Charta zu beurteilen ist. Bei der Beurteilung von Notwendigkeit und Verhältnismäßigkeit muss der Gesetzgeber insbesondere präzise angeben, in welchem Umfang die vorgeschlagene Maßnahme die Verarbeitung personenbezogener Daten vorsieht, und welche(s) das/die Ziel(e) und der/die konkrete(n) Zweck(e) der Maßnahme ist/sind. Auch die Probleme, die die Maßnahme lösen soll, sollten ausreichend und klar dargestellt werden, und ihre Existenz sollte durch objektive Beweise belegt werden. Schließlich sollte nachgewiesen werden, dass sich der/die angestrebte(n) Zweck(e) nicht mit anderen, weniger einschneidenden Maßnahmen erreichen lässt/lassen.[14]

17 Wir halten fest, dass in der ersten Folgenabschätzung von vier Hauptmängeln die Rede ist, die in der Mitteilung von 2016 unterstrichen wurden, nämlich
- suboptimale Funktionen bestehender Informationssysteme;
- bestehende Lücken in der Datenverwaltungsarchitektur der EU;
- die komplexe Landschaft unterschiedlich geregelter Informationssysteme und
- die Fragmentierung der Datenverwaltungsarchitektur für die Grenzkontrolle und -sicherung.

18 Interoperabilität zwischen Systemen wird dann als wesentlich für die Beseitigung der genannten Mängel bezeichnet, insbesondere im Hinblick auf
- den Mangel an vollständigen und genauen Daten;
- den Mangel an schnellem und reibungslosem Zugang zu allen Informationen;
- die Bedingungen, die Strafverfolgungsbehörden erfüllen müssen, um Zugang zu Datenbanken aus anderen Bereichen zu erhalten, und
- Identitätsbetrug.

19 In der ersten Folgenabschätzung werden zwar gewisse Probleme aufgeführt, doch wird dort nicht im Einzelnen beschrieben, worum es genau geht. Häufig wird nicht klar, ob es sich um ein rechtliches oder ein technisches Problem oder eine Kombination von beidem handelt. Was ist beispielsweise genau unter „Mangel an schnellem und reibungslosem Zugang zu allen Informationen“ zu verstehen? Ist es eine rechtliche Frage (erlaubt also die geltende Rechtsgrundlage einem Nutzer keinen Zugriff auf bestimmte Daten) oder ist es eine technische Frage (ist z. B. die Antwortzeit des Systems zu lang) oder vielleicht eine Kombination von beidem? Je nach Problemstellung kann die für seine Beseitigung angemessene Lösung verschieden ausfallen, insbesondere im Hinblick auf die Verarbeitung von Daten. Ohne eine klare und hinreichend genaue Beschreibung von Problemen und Bedarf ist nur schwer zu gewährleisten, dass die vorgeschlagenen Maßnahmenoptionen (also Einrichtung eines europäischen Suchportals, der BMS oder ein gemeinsamer Speicher) angemessen, verhältnismäßig und auf den ermittelten Bedarf wirklich zugeschnitten sind.

20 Mit anderen Worten: Nur mit einer klaren Beschreibung der beim Erreichen der angestrebten Ziele auftretenden Probleme ist der EU-Gesetzgeber in der Lage, im Einklang mit dem Datenschutzrecht die angemessensten rechtlichen und technischen Lösungen zu finden. Technologie sollte stets politischen Konzepten und dem Nutzerbedarf dienen, nicht umgekehrt. Was technisch machbar ist, muss nicht unbedingt rechtlich gerechtfertigt oder ethisch wünschenswert sein. Wie es in der Präambel der Datenschutz-Grundverordnung heißt: „Die Verarbeitung personenbezogener Daten sollte im Dienste der Menschheit stehen“.[15]

3.3 Zweckbindung im Hinblick auf Migration, Asyl sowie polizeiliche und justizielle Zusammenarbeit

21 Wir möchten betonen, dass es bei der Erwägung einer Interoperabilität von Informationssystemen auch darauf ankommt, den politischen Kontext zu berücksichtigen, in dem die einzelnen Systeme eingerichtet wurden. Eine Interoperabilität, wie sie sich die Kommission vorstellt, hätte Auswirkungen auf Instrumente, die zur Unterstützung der Politik in den Bereichen i) Grenzkontrollen, Asyl und Einwanderung sowie ii) polizeiliche Zusammenarbeit und iii) justizielle Zusammenarbeit aufgebaut wurden. In politischen Prozessen in der EU wird der Trend immer deutlicher, Migrationssteuerung und

Sicherheitszwecke miteinander zu verquicken. Wir beobachten diesen Trend im Zusammenhang mit der Gewährung des Zugangs zu bestehenden Systemen für Strafverfolgungszwecke[16], mit dem Aufbau neuer Informationssysteme[17] oder mit der Ausdehnung der Zuständigkeiten einer bestehenden Einrichtung[18]. Wir befürchten, dass dadurch, dass Migration, innere Sicherheit und Terrorismusbekämpfung verstärkt als austauschbare Begriffe verwendet werden, die Grenzen zwischen Migrationssteuerung und Terrorismusbekämpfung zu verwischen drohen. Dies könnte sogar dazu führen, dass Terroristen und Ausländer gleichgesetzt werden.

22 Zwar wurde bei der Entwicklung der bestehenden Systeme an eine getrennte Anwendung in der europäischen Migrations- bzw. Strafverfolgungspolitik gedacht, doch mögen zugegebenermaßen Synergien zwischen Maßnahmen und Zielen in den Bereichen Migration und polizeiliche Zusammenarbeit bestehen. Dessen ungeachtet sollte berücksichtigt werden, dass Migration auf der einen und polizeiliche Zusammenarbeit auf der anderen Seite noch immer zwei verschiedene Politikbereiche und Ziele öffentlichen Interesses sind, die unterschiedliche Rechtsgrundlagen im AEUV haben und jeweils spezifische Ziele verfolgen, die sauber voneinander getrennt werden müssen. Dies kann sich auf die Beurteilung der Kompatibilität von Zwecken der Datenverarbeitung auswirken, die die Kommission mit Blick auf den anstehenden Legislativvorschlag zu berücksichtigen hat.

3.4 Die vorgeschlagenen Optionen für Interoperabilität

23 Schon jetzt möchten wir den EU-Gesetzgeber auf einige Datenschutzprobleme hinweisen, die sich bei einigen der derzeit in der Diskussion stehenden spezifischen Lösungen ergeben könnten, wobei wir davon ausgehen, dass

- der anstehende Legislativvorschlag ganz klar die ermittelten Zwecke, Ziele und Bedürfnisse als ein Ergebnis der aufgetretenen Probleme beschreibt und
- ausreichend Informationen vorgelegt werden, damit die Notwendigkeit und Verhältnismäßigkeit der gewählten Lösungen beurteilt werden kann.[19]

Bei diesen Problemen handelt es sich insbesondere um die Bedingungen für den Zugang zu den Datenbanken, die Nutzung bestehender Datenbanken für neue/zusätzliche Zwecke und die Datensicherheit.

Neuer Zugriff (neue Modalitäten des Zugriffs)

24 Die erste Folgenabschätzung besagt, dass in Fällen, in denen Endnutzer keinen Zugriff auf bestimmte Daten in den Zentralsystemen haben, das europäische Suchportal (mit alphanumerischen Daten) und der gemeinsame biometrische Dienst (mit biometrischen Daten) Zugriff über die Angabe „Treffer“ bzw. „kein Treffer“ bietet; hier wird also nur angezeigt, dass in den zugrunde liegenden Systemen relevante Daten vorhanden sind, ohne dass die Daten jedoch offengelegt werden.

25 Je nach dem/den Ziel(en) eines solchen neuen Funktionsmerkmals könnte es gelten als

- eine neue Form der Verarbeitung personenbezogener Daten, also als *ein neuer Zugriff*: Die Behörde darf nicht auf die in einem bestimmten System erfassten Daten zugreifen, würde aber erfahren, ob das System Informationen über eine bestimmte Person enthält oder nicht;
- eine Änderung der *für die Datenverarbeitung geltenden Bedingungen* (in diesem Fall der Bedingungen für den Zugriff auf personenbezogene Daten): Die Behörde bekommt

Zugriff, aber nur unter bestimmten Voraussetzungen (die aus dem Blickwinkel der Grundrechte als *Garantien* fungieren könnten). Mit dem vorgeschlagenen System von „Treffer“ oder „kein Treffer“ hätte eine Behörde direkten Zugriff auf eine Datenbank, mit dem sie überprüfen könnte, ob die Datenbank Angaben zu einer bestimmten Person enthält. Als Antwort erhielte sie jedoch nur ein Ja („Treffer“) oder Nein („kein Treffer“). Im Falle einer positiven Antwort („Treffer“) müsste die Behörde bestimmte Bedingungen erfüllen, um Zugriff auf nähere Informationen zu erhalten (z. B. die Genehmigung einer unabhängigen Behörde).

26 Für den Fall des oben beschriebenen *neuen Zugriffs* muss unbedingt klargestellt werden, dass das Vorliegen (oder das Fehlen) eines „Treffers“ schon personenbezogene Daten sind, selbst wenn nur Mindestinformationen vorliegen (z. B. in einem bestimmten System bekannt oder unbekannt), da es sich um Informationen über eine Person handelt (ist die betreffende Person z. B. Gegenstand einer Ausschreibung im Schengener Informationssystem oder nicht). Folglich darf ein Nutzer, der keinen Zugriff auf die in einem bestimmten System gespeicherten Daten hat, auch keinen Zugriff auf die Angabe „Treffer“ bzw. „kein Treffer“ erhalten, da selbst diese minimalen Informationen als personenbezogene Daten gelten. Wir fragen uns im Übrigen, welchen Nutzen ein solches Merkmal haben sollte, da das Wissen, dass Informationen vorliegen („Treffer“) ohne die Möglichkeit eines Zugriffs auf den ganzen Datensatz in der Regel in einem Entscheidungsfindungsprozess kaum weiterhelfen dürfte und im Widerspruch zum Datenschutzgrundsatz der Datenqualität stehen würde (dass nämlich nur die personenbezogenen Daten verarbeitet werden dürfen, die für den angegebenen Zweck erforderlich sind).

27 Mit Blick auf das System „Treffer“ bzw. „kein Treffer“ als *Bedingung für den Zugriff* geht der EDSB davon aus, dass mit diesem System einige Garantien geboten werden könnten (also beschränkter Zugriff), die eine oder mehrere der Bedingungen ersetzen würden, die Strafverfolgungsbehörden heute zu erfüllen haben, wenn sie auf Datenbanken zugreifen, die nicht zum Bereich Strafverfolgung gehören.

28 Derzeit muss eine Strafverfolgungsbehörde, die auf Datenbanken außerhalb des Bereichs Strafverfolgung zugreifen möchte, mehrere Bedingungen erfüllen (z. B. Zugriff in einem konkreten Fall benötigt, begründeter Verdacht, vorherige Abfrage nationaler Datenbanken usw.). Dazu gehört auch die vorherige Genehmigung durch eine andere Behörde, die unabhängig und für die Prävention, Aufdeckung oder Untersuchung terroristischer oder sonstiger schwerwiegender Straftaten verantwortlich ist. Bevor eine solche Behörde eine Genehmigung erteilt, überprüft sie, ob alle in der Rechtsgrundlage für das betreffende Informationssystem aufgeführten Bedingungen für den Zugriff erfüllt sind.

29 Im Bericht der HLEG findet sich die Anregung, dass es Strafverfolgungsbehörden zur Beantwortung der Frage, ob ein Großsystem Informationen über eine Person enthält (oder nicht), erlaubt sein sollte, Informationssysteme aus anderen Bereichen als der Strafverfolgung ohne vorherige Genehmigung abzufragen. Bei anderen Zwecken (wie beispielsweise der Rekonstruktion des Reiseverlaufs eines bekannten Verdächtigen im Rahmen einer bestimmten Ermittlung) wäre die Genehmigung weiterhin vorgeschrieben.

30 Es sei an dieser Stelle darauf hingewiesen, dass IT-Großsysteme der EU - wie das Visa-Informationssystem oder Eurodac - für die Bereiche Migration und Asyl eingerichtet wurden. Die Möglichkeit des Zugangs zu diesen Datenbanken für

Strafverfolgungsbehörden wurde erst später hinzugefügt, und auch nur unter bestimmten Bedingungen (Garantien), um unangemessene Auswirkungen auf die betreffenden Personen zu begrenzen. Jede potenzielle Lockerung dieser bestehenden Bedingungen müsste daher genau begründet werden und würde eine gründliche und umfassende Analyse aller verbleibenden und/oder neuen Garantien im Hinblick auf die Notwendigkeit und Verhältnismäßigkeit einer solchen Lockerung erfordern. Um insbesondere ein hohes Schutzniveau gegen möglichen Missbrauch zu erhalten, sollten verringerte Garantien von Ex-ante-Kontrollen zumindest mit verstärkten Ex-post-Kontrollen einhergehen.

Neue Verwendungen von Daten

31 Die erste Folgenabschätzung besagt, dass der gemeinsame Dienst für den Abgleich biometrischer Daten („BMS“) einen Abgleich der in den verschiedenen Datenbanken gespeicherten biometrischen Daten ermöglichen soll, während im gemeinsamen Speicher für Identitätsdaten alphanumerische Daten (wie Namen und Geburtsdaten) aus den verschiedenen Informationssystemen für Grenzmanagement und Sicherheit zusammengeführt werden sollen. Beim kombinierten Einsatz von BMS und gemeinsamem Speicher für Identitätsdaten ließe sich mit Hilfe der gleichen, in den verschiedenen IT-Großsystemen gespeicherten biometrischen Daten ermitteln, ob jemand mit mehreren Identitäten auftritt, und könnte auf diese Weise gegen Identitätsbetrug vorgegangen werden.

32 Es wäre zu bedenken, dass die Verwendung eindeutiger Kennungen in Kombination mit technischen Möglichkeiten zur Erfassung aller verfügbaren Informationen über Personen aus anderen Informationssystemen einer neuen Form der Verarbeitung personenbezogener Daten gleichkäme, die angemessen und ausreichend begründet werden muss (siehe Abschnitte 3.1 und 3.2).

33 Darüber hinaus sind die Informationssysteme, deren Daten in den gemeinsamen Speicher für Identitätsdaten eingehen würden, für andere Zweck als die Bekämpfung von Identitätsbetrug aufgebaut worden, die einen neuen Zweck der Datenverarbeitung darstellt. In diesem Zusammenhang sehen wir das Risiko einer „Zweckentfremdung“ (also einer allmählichen Ausdehnung der Nutzung eines Systems oder einer Datenbank über den/die Zweck(e) hinaus, zu dem/denen es/sie ursprünglich konzipiert wurde). Wie bei jeder Initiative, die potenziell weitere Verwendungen von Daten oder Systemen über das hinaus ermöglichen würde, was ursprünglich im Gesetz vorgesehen war, raten wir hier zur Vorsicht. Das Argument, wonach die Daten sowieso schon erhoben sind und somit genauso gut auch für andere Zwecke verwendet werden können, kann nicht unwidersprochen hingenommen werden, da eine solche neue Form der Verarbeitung größere Auswirkungen auf die Betroffenen haben kann.

34 Schließlich möchten wir die Gelegenheit nutzen und noch Klarstellendes zum Grundsatz der Datenminimierung sagen, der häufig missverstanden wird. So heißt es beispielsweise in der Mitteilung von 2016, dass die Speicherung ein und derselben Daten in verschiedenen Informationssystemen dem Grundsatz der Datenminimierung zuwider läuft. In der ersten Folgenabschätzung heißt es hierzu weiter, ein gemeinsamer Speicher für Identitätsdaten würde durch die Vermeidung der Doppelerfassung von Daten zu mehr Effizienz beitragen. Eine Vermeidung der Doppelerfassung von Daten allein gewährleistet jedoch nicht die Datenminimierung. Der im Datenschutzrecht verankerte Grundsatz der Datenminimierung verlangt zuallererst, dass sich die Erhebung und Verarbeitung von Daten auf die Daten

beschränkt, die für die angestrebten Zwecke angemessen, relevant und notwendig sind.[20] Das bedeutet in der Praxis, dass das gemeinsame Nutzen von Daten in Datenbanken, die dieselben Daten verarbeiten, für die Umsetzung des Grundsatzes der Datenminimierung nicht zwangsläufig ausreicht.

Neue Herausforderungen bezüglich der Sicherheit

35 Wir möchten darauf hinweisen, dass Interoperabilität - wie sie bisher von der Kommission angedacht wurde - grundlegende Veränderungen an der bestehenden Architektur von IT-Großsystemen mit sich bringen würde, nämlich den Übergang von einem geschlossenen Umfeld zu einem gemeinsamen Umfeld mit Verbindungen zwischen den verschiedenen Systemen. Dadurch entstünden neue Sicherheitsrisiken. Nehmen wir als Beispiel das europäische Suchportal: Hier würden solche Risiken beispielsweise aufgrund der Tatsache auftreten, dass ein Angreifer lediglich einen einzigen Zugangspunkt angreifen müsste (und nicht mehrere Zugangspunkte, also in jedem einzelnen Informationssystem), um Zugang zu mehreren IT-Großsystemen zu erhalten.

36 Es ist daher unbedingt geboten, die Konsequenzen der verschiedenen Optionen für das Erreichen von Interoperabilität für die Informationssicherheit sorgfältig zu analysieren. Eine umfassendes Management der Risiken für die Informationssicherheit im Einklang mit Artikel 22 der Verordnung (EG) Nr. 45/2001 sowie Leitlinien des EDSB dürften erforderlich sein, bevor irgendwelche Änderungen vorgenommen werden, die möglicherweise die Sicherheit aller Systeme berühren.[21]

4 Schlussfolgerungen

37 Wir unterstützen Interoperabilität, sofern sie sorgfältig durchdacht und im Einklang mit den grundlegenden Erfordernissen der Notwendigkeit und Verhältnismäßigkeit umgesetzt wird. Interoperabilität kann dann ein hilfreiches Instrument zur Deckung berechtigter Erfordernisse zuständiger Behörden sein, die IT-Großsysteme der EU nutzen, und kann unter anderem die Informationsweitergabe verbessern.

38 Interoperabilität gilt zwar häufig als rein technisches Konzept, doch kann es im vorliegenden Kontext nicht von den Fragen getrennt werden, ob der Datenaustausch wirklich erforderlich, politisch wünschenswert oder rechtlich gerechtfertigt ist.

39 Aus dem Blickwinkel der Grundrechte hätte die Kommission unserer Auffassung nach Interoperabilität als Instrument konzipieren können, das lediglich die Nutzung der Systeme erleichtert und nur die derzeit geltenden Vorschriften wirksamer und effizienter macht. Wir gehen allerdings davon aus, dass die Kommission sie möglicherweise auf neue Möglichkeiten des Austauschs oder Abgleichs von Daten ausdehnen möchte. Dies brächte neue Formen der Datenverarbeitung mit sich, die durch die bestehenden Rechtsinstrumente nicht abgedeckt sind. Ihre Auswirkungen auf die Grundrechte auf Privatsphäre und Datenschutz müssen sorgfältig geprüft werden.

40 Es muss unbedingt berücksichtigt werden, dass die Einhaltung der EU-Datenschutzvorschriften über die Grundsätze des Datenschutzes durch Technikgestaltung /datenschutzfreundliche Voreinstellungen, die Verpflichtung zur Anwendung von

Sicherheitsmaßnahmen usw. hinausgeht und verlangt, dass zunächst einmal die Notwendigkeit und Verhältnismäßigkeit der Verarbeitung festgestellt wird.

41 In dem anstehenden Legislativvorschlag sollten insbesondere die Probleme klar umrissen werden, die die Interoperabilität lösen soll, damit eine angemessene Debatte aus dem Blickwinkel der Grundrechte geführt werden kann. Wir halten fest, dass die Kommission zwar gewisse Probleme identifiziert, doch nicht im Einzelnen beschreibt, worum es genau geht. Häufig wird nicht klar, ob es sich um ein rechtliches oder ein technisches Problem oder eine Kombination von beidem handelt. Je nach Problem kann die für seine Beseitigung angemessene Lösung verschieden ausfallen, insbesondere im Hinblick auf die Verarbeitung von Daten. Der Vorschlag sollte ebenfalls klare Aussagen dazu enthalten, für welche spezifischen Zwecke welche Kategorien personenbezogener Daten verarbeitet werden würden.

42 Folglich sind wir der Auffassung, dass eine vollständige Bewertung der Auswirkungen der Interoperabilität auf die Grundrechte auf Privatsphäre und Datenschutz unbedingt geboten ist, sobald nähere Einzelheiten zu der geplanten Initiative bekannt sind. Der anstehende Legislativvorschlag könnte in diesem Sinne eine Chance für die Gestaltung eines kohärenteren und schlüssigeren Rahmens bieten, die nicht ungenutzt verstreichen sollte.

Brüssel, den 17. November 2017

Giovanni BUTTARELLI

Endnoten

[1] Siehe beispielsweise den 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, COM(2016) 194 final; den 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, COM(2016) 731 final.

[2] Siehe beispielsweise das SIS-Legislativpaket, bestehend aus i) dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates 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, COM(2016) 882 final; ii) dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates 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, COM(2016) 883 final und iii) dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Nutzung des Schengener Informationssystems für die Rückkehr illegal aufhältiger Drittstaatsangehöriger, COM(2016) 881 final. Siehe auch den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Änderung der Verordnung (EU) Nr. 603/2013 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, 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, COM(2016) 272 final.

[3] Mitteilung der Kommission an das Europäische Parlament und den Rat „Solidere und intelligentere Informationssysteme für das Grenzmanagement und mehr Sicherheit“, 6. April 2016, COM(2016) 205 final.

[4] a.a.O., S. 17.

[5] Zwischenbericht des Vorsitzes der von der Europäischen Kommission eingesetzten hochrangigen Sachverständigengruppe „Informationssysteme und Interoperabilität“, Zwischenbericht des Vorsitzes der hochrangigen Sachverständigengruppe, Dezember 2016, abrufbar unter: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3435

[6] Abschlussbericht der von der Europäischen Kommission eingesetzten hochrangigen Sachverständigengruppe „Informationssysteme und Interoperabilität“, 11. Mai 2017, abrufbar unter: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3435

[7] Mitteilung der Kommission an das Europäische Parlament, den Europäischen Rat und den Rat, „Auf dem Weg zu einer wirksamen und echten Sicherheitsunion - Siebter Fortschrittsbericht“, 16. Mai 2017, COM(2017) 261 final.

[8] Schlussfolgerungen des Rates zum weiteren Vorgehen zur Verbesserung des Informationsaustauschs und zur Sicherstellung der Interoperabilität der EU-Informationssysteme, 8. Juni 2017: http://data.consilium.europa.eu/doc/document/ST-10151-2017-INIT/de/pdf.

[9] Öffentliche Konsultation und Folgenabschätzung sind abrufbar unter: https://ec.europa.eu/home-affairs/content/consultation-interoperability-eu-information-systems-borders-and-security_en.

[10] Vorläufige Tagesordnungen für anstehende Sitzungen der Kommission, http://ec.europa.eu/transparency/regdoc/rep/2/2017/EN/SEC-2017-415-F1-EN-MAIN-PART-1.PDF.

[11] Siehe Stellungnahme 6/2016 des EDSB zum zweiten Paket Intelligente Grenzen, Punkt III.3.d, S. 17 https://edps.europa.eu/sites/edp/files/publication/16-09-21_smart_borders_de.pdf.

[12] Erste Folgenabschätzung, S. 2.

[13] Siehe „Schritt 3“ des vom EDSB am 11. April 2017 herausgegebenen „Toolkit zur Beurteilung der Erforderlichkeit von Maßnahmen“, abrufbar unter: https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en_0.pdf.

[14] Siehe das vom EDSB am 11. April 2017 herausgegebene „Toolkit zur Beurteilung der Erforderlichkeit von Maßnahmen“, das die EU-Gesetzgeber bei der Erarbeitung und Prüfung von Maßnahmen unterstützen soll, in deren Rahmen personenbezogene Daten verarbeitet werden, und die dem Recht auf Privatsphäre und Datenschutz

sowie anderen in der Charta der Grundrechte der Europäischen Union verankerten Rechten und Freiheiten zuwiderlaufen könnten, abrufbar unter: https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en_0.pdf.

[15] 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), ABl. L 119 vom 4.5.2016, S. 1.

[16] Beschluss 2008/633/JI des Rates vom 23. Juni 2008 über den Zugang der benannten Behörden der Mitgliedstaaten und von Europol zum Visa-Informationssystem (VIS) für Datenabfragen zum Zwecke der Verhütung, Aufdeckung und Ermittlung terroristischer und sonstiger schwerwiegender Straftaten, ABl. L 218 vom 13.8.2008; 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 (Neufassung), ABl. L 180 vom 29.6.2013, S. 1.

[17] Siehe z. B. den 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, COM(2016) 194 final. Siehe ferner den 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, COM(2016) 731 final.

[18]Vorschlag für eine Verordnung über die Europäische Grenz- und Küstenwache und zur Aufhebung der Verordnung (EG) Nr. 2007/2004, der Verordnung (EG) Nr. 863/2007 und der Entscheidung 2005/267/EG des Rates, (COM(2015) 671 final).

[19] Siehe das vom EDSB am 11. April 2017 herausgegebene „Toolkit zur Beurteilung der Erforderlichkeit von Maßnahmen“, das die EU-Gesetzgeber bei der Erarbeitung und Prüfung von Maßnahmen unterstützen soll, in deren Rahmen personenbezogene Daten verarbeitet werden und die dem Recht auf Privatsphäre und Datenschutz sowie anderen in der Charta der Grundrechte der Europäischen Union verankerten Rechten und Freiheiten zuwiderlaufen könnten, abrufbar unter: https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en_0.pdf.

[20] Gemäß Artikel 5 Absatz 1 Buchstabe c der Datenschutz-Grundverordnung müssen personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein (Datenminimierung).

[21] Leitlinien zu Sicherheitsmaßnahmen für die Verarbeitung personenbezogener Daten, Artikel 22 der Verordnung (EG) Nr. 45/2001, https://edps.europa.eu/sites/edp/files/publication/16-03-21_guidance_isrm_en.pdf.