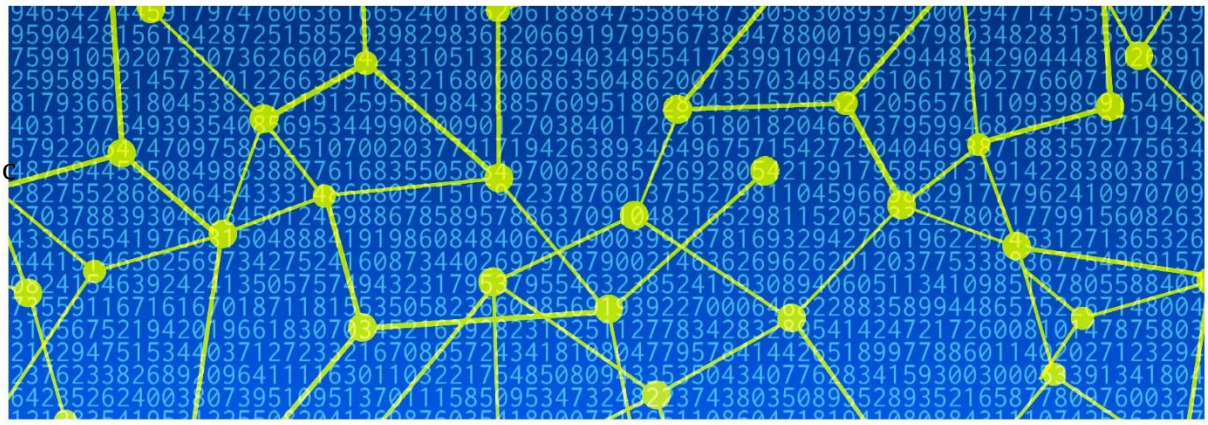

EUROPEAN DATA PROTECTION SUPERVISOR

Stellungnahme 3/2017

Stellungnahme des EDSB zu dem Vorschlag für ein Europäisches Reiseinformations- und -genehmigungs-system (ETIAS)

EDPS

6. März 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 der 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". Nach Auffassung des EDSB spielt die Erfüllung der Datenschutzauflagen eine zentrale Rolle für den Erfolg des künftigen Reiseinformations- und -genehmigungssystems.

Zusammenfassung

Aufgrund der Herausforderungen durch den Zustrom von Flüchtlingen und Migranten sowie von Sicherheitsüberlegungen, die durch die Anschläge in Paris, Brüssel und Nizza noch intensiviert wurden, hat die Grenzmanagementpolitik der EU in den vergangenen Jahren erhebliche Veränderungen erlebt. Die derzeitige Situation und die Notwendigkeit, die Sicherheit im Hoheitsgebiet der Mitgliedstaaten zu gewährleisten, war Anlass für die Kommission, mehrere Gesetzesinitiativen mit dem Ziel in die Wege zu leiten, die Kontrolle von in den Schengen-Raum einreisenden Personen zu verbessern.

Eine dieser Initiativen ist der Vorschlag für eine Verordnung über ein Europäisches Reiseinformations- und -genehmigungssystem („ETIAS"), der von der Kommission am 16. November 2016 vorgelegt wurde.

Der Vorschlag sieht vor, dass sich von der Visumpflicht befreite Reisende vor ihrer Ankunft an den Grenzen des Schengen-Raums einer Risikobewertung im Hinblick auf Risiken für die Sicherheit, Risiken durch irreguläre Migration und Risiken für die öffentliche Gesundheit zu unterziehen haben. Vorgenommen werden soll diese Bewertung mittels eines Abgleichs der vom Antragsteller bei ETIAS eingereichten Daten mit anderen EU-Informationssystemen, einer speziellen ETIAS-Überwachungsliste und Überprüfungsregeln. Ergebnis dieses Verfahrens ist die Erteilung – oder Verweigerung – einer automatisierten Genehmigung für die Einreise in die EU.

Mit dem ETIAS-Vorschlag scheint sich der EU-Gesetzgeber dem wachsenden Trend zur gemeinsamen Behandlung von Zwecken des Sicherheits- und Migrationsmanagements anzuschließen, ohne jedoch die substanziellen Unterschiede zwischen diesen beiden Politikbereichen zu berücksichtigen. Die Einrichtung des ETIAS hätte erhebliche Auswirkungen auf den Schutz personenbezogener Daten, da verschiedene Arten von Daten, die ursprünglich zu völlig unterschiedlichen Zwecken erhoben wurden, nun einem breiteren Spektrum von Behörden (nämlich Einwanderungsbehörden, Grenzschutz, Gefahrenabwehr- und Strafverfolgungsbehörden usw.) zugänglich gemacht werden. Der EDSB ist daher der Auffassung, dass eine Abschätzung der Auswirkungen des Vorschlags auf das Recht auf Privatsphäre und das Recht auf den Schutz personenbezogener Daten, wie sie in der Charta der Grundrecht der EU verankert sind, vorgenommen werden muss, bei der eine Bestandsaufnahme aller auf EU-Ebene bestehenden Maßnahmen für Migrations- und Sicherheitsziele erfolgt.

Des Weiteren ruft der ETIAS-Vorschlag Bedenken im Hinblick auf das Verfahren zur Ermittlung eventuell durch den Antragsteller verursachter Risiken hervor. Vor diesem Hintergrund sollte der Definition solcher Risiken besondere Aufmerksamkeit geschenkt werden. In Anbetracht der Tatsache, dass die Konsequenz für eine natürliche Person die Verweigerung der Einreise sein könnte, sollten die beurteilten Risiken im Gesetz genau definiert werden. Der EDSB stellt ferner die Existenz der ETIAS-Überprüfungsregeln in Frage. Der EDSB geht davon aus, dass das Ziel des Gesetzgebers darin besteht, ein automatisches Aussortieren von von der Visumpflicht befreiten Drittstaatsangehörigen zu ermöglichen, die im Verdacht stehen, solche Risiken darzustellen. Dessen ungeachtet wirft Profilung genauso wie jede andere Form der auf natürliche Personen angewandten computergestützten Datenauswertung schwerwiegende technische, rechtliche und ethische Fragen auf. Der EDSB fordert daher überzeugende Beweise dafür, dass der Einsatz von Profiling-Tools für die Zwecke des ETIAS notwendig ist.

Darüber hinaus hinterfragt der EDSB die Relevanz der Erhebung und Verarbeitung von Gesundheitsdaten, wie sie im Vorschlag geplant ist. Er fordert eine bessere Begründung der vorgeschlagenen Speicherfrist für die Daten sowie der Notwendigkeit eines Zugriffs auf die Daten für nationale Gefahrenabwehr- und Strafverfolgungsbehörden und Europol.

Schließlich formuliert er Empfehlungen beispielsweise zur Aufteilung der Aufgaben und Verantwortlichkeiten auf die verschiedenen beteiligten Stellen sowie zur Architektur und Informationssicherheit des ETIAS.

INHALT

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],

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[2], 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[3] –

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

I. EINLEITUNG

1. Die Initiative der Europäischen Kommission zur Einrichtung eines Europäischen Reiseinformations- und -genehmigungssystems (nachstehend „ETIAS“ genannt) geht zurück auf eine Mitteilung aus dem Jahr 2008 mit dem Titel „Vorbereitung der nächsten Schritte für die Grenzverwaltung in der Europäischen Union“[4]. In dieser Mitteilung schlug die Kommission neue Instrumente für das künftige Management europäischer Grenzen vor, insbesondere das Einreise-/Ausreisesystem („EES“) und das Registrierungsprogramm für Reisende („RTP“), und erwog zum ersten Mal die Einführung von ETIAS, damals noch als System der EU zur elektronischen Erteilung von Reisebewilligungen („ESTA“) bezeichnet. Noch im gleichen Jahr gab der EDSB vorläufige Kommentare[5] zu dieser Mitteilung heraus.

2. Im Februar 2011 veröffentlichte die Kommission eine Studie[6], in der vier Optionen für die Einführung eines EU-ESTA analysiert wurden. Die Studie kam zu dem Schluss, dass seinerzeit die Voraussetzungen nicht gegeben waren, die den Aufbau eines EU-ESTA gerechtfertigt hätten. In einer Mitteilung über intelligente Grenzen[7] aus dem Jahr 2012 vertrat die Kommission die Ansicht, die Einrichtung eines EU-ESTA solle einstweilen verworfen werden, kündigte jedoch ihre Absicht an, die Arbeiten am EES und am RTP fortzusetzen.

3. In der Mitteilung[8] „Solidere und intelligentere Informationssysteme für das Grenzmanagement und mehr Sicherheit“ vom 6. April 2016 kündigte die Kommission eine Prüfung der Notwendigkeit, technischen Machbarkeit und Verhältnismäßigkeit der Einrichtung eines künftigen Europäischen Reiseinformations- und -genehmigungssystems an. Noch im gleichen Jahr führte die Kommission eine Machbarkeitsstudie durch, die sich

an drei anderen weltweit bereits bestehenden Reisegenehmigungssystemen orientierte, nämlich dem ESTA in den USA, dem eTA in Kanada und dem eVisitor in Australien.

4. Am 16. November veröffentlichte die Kommission den Abschlussbericht der Machbarkeitsstudie[9] (nachstehend „Machbarkeitsstudie von 2016“) sowie den ETIAS-Vorschlag (nachstehend „der Vorschlag“).

5. Der EDSB begrüßt, dass er vor der Annahme des Vorschlags von den Dienststellen der Kommission informell konsultiert wurde. Er bedauert allerdings, dass aufgrund der sehr kurzen Frist und der Bedeutung und Komplexität des Vorschlags es seinerzeit nicht möglich war, einen sinnvollen Beitrag zu leisten.

II. ZIEL DES VORSCHLAGS

6. Der EDSB entnimmt dem Vorschlag und den ihn begleitenden Dokumenten, dass ETIAS ein automatisiertes IT-System ist, das für den Zweck geschaffen wird, Risiken durch Migration, Risiken für die Sicherheit und Risiken für die Gesundheit zu ermitteln, die von von der Visumpflicht befreiten Besuchern ausgehen, die in den Schengen-Raum reisen. Er hält fest, dass Zugriff auf die in ETIAS verarbeiteten Daten auch nationale Gefahrenabwehr- und Strafverfolgungsbehörden und Europol haben, wenn dies für die Verhütung, Aufdeckung und Untersuchung terroristischer und sonstiger schwerer Straftaten erforderlich ist.

7. Nach dem Vorschlag müssen alle von der Visumpflicht befreiten Drittstaatsangehörigen vor Antritt ihrer Reise einen Datensatz in einen Online-Antrag eingeben. Bei der Überprüfung und Bewertung der von den von der Visumpflicht befreiten Reisenden eingegebenen Informationen vor der Erteilung oder Verweigerung einer Reisegenehmigung nimmt das System einen automatisierten Abgleich jedes Antrags vor, und zwar mit:
   - anderen Informationssystemen der EU – dem Schengener Informationssystem („SIS“), dem Visa-Informationssystem („VIS“), Europol-Daten, der Interpol-Datenbank für gestohlene und verlorene Reisedokumente („SLTD“) sowie möglicherweise der Eurodac-Datenbank, dem künftigen Europäischen Strafregisterinformationssystem („ECRIS“) für Drittstaatsangehörige und dem künftigen EES,
   - einer speziellen ETIAS-Überprüfungsliste, die von Europol erstellt wird und aus Daten über Personen besteht, die verdächtigt werden, eine Straftat begangen oder sich daran beteiligt zu haben, oder über Personen, bei denen tatsächliche Anhaltspunkte oder hinreichende Gründe für die Annahme bestehen, dass sie Straftaten begehen werden,
   - und Überprüfungsregeln, die innerhalb des ETIAS-Zentralsystems festgelegt sind.

8. Ergibt die automatisierte Verarbeitung keinen Treffer, stellt das System automatisch eine Reisegenehmigung aus. Ergibt sie einen oder mehrere Treffer, wird der Antrag manuell von der nationalen ETIAS-Stelle des Mitgliedstaats bearbeitet, in den der Reisende laut seinem Antrag zuerst einreisen will. Aufgabe der nationalen ETIAS-Stelle ist es dann, das Risiko der irregulären Migration, das Risiko für die Sicherheit oder für die öffentliche Gesundheit zu bewerten und zu entscheiden, ob eine Reisegenehmigung ausgestellt oder verweigert wird.

III. HAUPTEMPFEHLUNGEN

1. Auswirkungen des ETIAS auf Privatsphäre und Datenschutz

9. Der EDSB stellt fest, dass es immer mehr politische Maßnahmen der EU in den Bereichen Sicherheit und Migration gibt. In seiner Rolle als Berater des Gesetzgebers ist der EDSB nicht *a priori* für oder gegen eine Maßnahme, stellt aber die Frage in den Mittelpunkt, inwieweit die Entscheidung des Gesetzgebers durch die Grundsätze des Datenschutzes eingeschränkt wird, und falls dem so sein sollte, ob dies mit ihnen im Einklang steht.

10. Der EDSB erinnert daran, dass das Recht auf den Schutz personenbezogener Daten, wie es in Artikel 8 der Charta der Grundrechte der Europäischen Union (nachstehend „die Charta“) verankert ist, für jede natürliche Person gilt, deren Daten von einem Verantwortlichen in der EU verarbeitet werden, und dies unabhängig davon, ob sie EU-Bürger, Migrant (irregulär oder nicht), Asylbewerber oder ein Mensch ist, für den die Unschuldsvermutung gilt. Im Einklang mit den in Artikel 52 Absatz 1 der Charta verankerten Grundsätzen der Notwendigkeit und Verhältnismäßigkeit dürfen Eingriffe in das Recht auf den Schutz personenbezogener Daten oder Einschränkungen dieses Rechts nur vorgenommen werden, wenn sie erforderlich sind und dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen. Der EDSB unterstreicht, dass diese Grundsätze hochrangige rechtliche Vorgaben des EU-Rechts sind und als solche unausweichlich der Überprüfung durch den Gerichtshof der EU unterliegen.

11. Zunächst einmal begrüßt der EDSB, dass dem Datenschutz im Vorschlag durchgehend Aufmerksamkeit geschenkt wird. Insbesondere begrüßt er die Angleichung an die Definitionen in der Datenschutz-Grundverordnung[10], der Richtlinie für die Bereiche Polizei und Justiz[11] und der Verordnung (EG) Nr. 45/2001 (Artikel 3 Absätze 2, 3 und 4); das Angebot an Schulungen zu Datensicherheit und Datenschutz für die Mitarbeiter der Europäischen Agentur für die Grenz- und Küstenwache, die in der ETIAS-Zentralstelle arbeiten, und die Mitarbeiter der nationalen ETIAS-Stellen, bevor sie die Genehmigung zur Verarbeitung der im ETIAS-Zentralsystem erfassten Daten erhalten (Artikel 65 Absatz 2 und Artikel 66 Absatz 3); den Verweis auf die für die verschiedenen Akteure geltenden Datenschutzrechtsrahmen (Artikel 49) und das Verbot der Übermittlung und Weiterübermittlung von ETIAS-Daten an Drittländer, internationale Organisationen und private Stellen innerhalb oder außerhalb der EU (Artikel 55).

12. Der Begründung und den Begleitdokumenten zu dem Vorschlag ist zu entnehmen, dass das ETIAS in der jetzt vorgeschlagenen Form unter anderem dazu beitragen soll, irreguläre Migration zu verhindern, für mehr innere Sicherheit zu sorgen und die öffentliche Gesundheit zu schützen. In diesem Zusammenhang hält der EDSB fest, dass der Vorschlag den Aufbau eines weiteren Systems im Bereich Einwanderung und Sicherheit bedeutet, das die Erhebung von deutlich mehr Daten (einschließlich Gesundheitsdaten und justizielle Daten) über Drittstaatsangehörige mit sich bringt. Der EDSB erinnert daran, dass sowohl die Notwendigkeit als auch die Verhältnismäßigkeit dieser Regelung insgesamt zu bewerten sind, und zwar unter Berücksichtigung der in der EU bereits bestehenden Systeme, der Art der Daten (einschließlich justizielle Daten und Gesundheitsdaten) und des Ausmaßes der geplanten Verarbeitung (alle von der Visumpflicht befreiten Drittstaatsangehörigen, die in den Schengen-Raum reisen).

13. Der EDSB weist darauf hin, dass dem Vorschlag keine Datenschutzfolgenabschätzung beigefügt ist, in der verschiedene Optionen geprüft werden, mit denen sich die angegebenen Ziele erreichen lassen, und zwar unter Berücksichtigung aller Maßnahmen auf EU-Ebene im gleichen Bereich und mit einer Bewertung der Auswirkungen der einzelnen Optionen auf (die Grundrechte) natürliche(r) Personen. **Der EDSB unterstreicht, dass es aufgrund der fehlenden Datenschutzfolgenabschätzung, die eine grundlegende Voraussetzung darstellt, nicht möglich ist, die Notwendigkeit und Verhältnismäßigkeit des ETIAS in der derzeit vorgeschlagenen Form vollständig zu beurteilen.** Dessen ungeachtet geht der EDSB aber auf einige Punkte ein, die in dieser Datenschutzfolgenabschätzung zu prüfen wären, wie:

1) die voneinander getrennten Politikbereiche Einwanderung und Sicherheit

14. Der EDSB stellt fest, dass Migrationsmanagement und Sicherheitszwecke zunehmend miteinander verbunden werden, wenn es um die Gewährung von Zugang zu bestehenden Systemen für Gefahrenabwehr- und Strafverfolgungszwecke (z. B. VIS und Eurodac[12]), den Aufbau neuer Informationssysteme (z. B. der Vorschlag für ein Einreise-/Ausreisesystem[13]) oder die Erweiterung der Kompetenzen einer bestehenden Einrichtung (z. B. der Europäischen Grenz- und Küstenwache[14]) geht.

15. Durch die gemeinsame Behandlung von irregulärer Einwanderung und Sicherheitszielen und die Schaffung einer einzigen Datenbank, die Daten sowohl zu Migration als auch zu Straftaten enthält, fügt sich der ETIAS-Vorschlag in diesen aktuellen Trend ein. Dies wirkt sich auf den Datenschutz aus, da mehr personenbezogene Daten erhoben und von verschiedenen Behörden (Einwanderungsbehörden, Grenzschutz, Gefahrenabwehr- und Strafverfolgungsbehörden usw.) abgerufen werden. Ferner besteht möglicherweise die Gefahr einer Überschneidung von Aufgaben und Datenverarbeitung, da nach dem Vorschlag sowohl die Europäische Agentur für die Grenz- und Küstenwache (nachstehend „EAGK“) als auch Europol – in gewissem Umfang – an der Bewertung von Risiken für die Sicherheit beteiligt sein werden. Der EDSB weist darauf hin, dass es durchaus Synergien zwischen Migration und innerer Sicherheit geben kann, dass es sich hierbei jedoch um zwei voneinander getrennte Bereiche der öffentlichen Ordnung mit unterschiedlichen Zielsetzungen und Hauptakteuren handelt.

2) Die Gefahr einer unausgewogenen Behandlung von von der Visumpflicht befreiten und von visumpflichtigen Reisenden

16. Der EDSB stellt die Frage in den Raum, ob der Vorschlag nicht für von der Visumpflicht befreite Reisende eine stärker in die Privatsphäre eindringende Regelung vorsieht als für visumpflichtige Reisende, denn im ETIAS[15] werden mehr Daten zentral auf EU-Ebene gespeichert als im VIS. Das hat zur Folge, dass von verschiedenen Behörden mit Zugang zum ETIAS auch mehr Daten abgerufen werden können. Im Übrigen merkt der EDSB an, dass Daten des Antragstellers auf eine elektronische Reisegenehmigung mit spezifischen Risikoindikatoren und einer Überprüfungsliste abgeglichen werden, die für die Erteilung eines Visums nicht verwendet werden.

3) Die Redundanz von ETIAS mit API und PNR Datenverarbeitung

17. Des Weiteren hinterfragt der EDSB die Redundanz des ETIAS mit erweiterten Fluggastdaten (Advanced Passenger Information – API) und Fluggastdatensätzen

(Passenger Name Records – PNR), die bei von der Visumpflicht befreiten Reisenden bereits erhoben werden, bevor sie den Schengen-Raum erreichen. Der EDSB hält fest, dass bei allen mit dem Flugzeug reisenden von der Visumpflicht befreiten Drittstaatsangehörigen ein Großteil der vom ETIAS zu erhebenden Daten bereits als API- und PNR-Daten zwecks Beurteilung von Passagieren vor ihrer Ankunft im Schengen-Hoheitsgebiet erhoben wurde (sobald das System seinen Betrieb aufgenommen haben wird). Der EDSB fragt sich, ob das ETIAS nicht in diesem Zusammenhang vorliegende Informationen ein zweites Mal erhebt.

18. Zusammenfassend **unterstreicht** der EDSB, **dass bei einer Datenschutzfolgenabschätzung des ETIAS eine Bestandsaufnahme aller auf EU-Ebene ergriffenen Maßnahmen in den Bereichen Migration und Sicherheitsziele vorgenommen und deren konkrete Umsetzung, Wirksamkeit und Auswirkung auf die Grundrechte natürlicher Personen gründlich analysiert werden sollten, bevor neue Systeme geschaffen werden, in denen wieder personenbezogene Daten verarbeitet werden. Bei dieser Analyse sollte dem Politikbereich, in dem diese Maßnahmen gelten, und der jeweiligen Rolle der wichtigsten beteiligten Akteure Rechnung getragen werden.**

2. Festlegung der Ziele des ETIAS

19. Der EDSB ruft in Erinnerung, dass nach dem Grundsatz der Zweckbindung, einem Kernelement des Datenschutzes, personenbezogene Daten für festgelegte, eindeutige und rechtmäßige Zwecke erhoben werden müssen. Der/die Zweck(e) muss/müssen so detailliert beschrieben sein, dass klar ist, welche Art von Verarbeitung für den festgelegten Zweck erfolgt. Nur mit genau festgelegten Zwecken ist eine korrekte Bewertung der Verhältnismäßigkeit und Angemessenheit der erhobenen personenbezogenen Daten möglich.

20. Der EDSB unterstreicht ferner, dass eine Festlegung der Zwecke nicht nur aus dem Blickwinkel des Datenschutzes von grundlegender Bedeutung ist, sondern auch für die Gewährleistung der Effizienz des Systems wesentlich ist: Wie sollte eine zuständige Behörde beurteilen können, ob eine natürliche Person ein Risiko durch irreguläre Migration und/oder ein Risiko für die Sicherheit darstellt, wenn nicht klar definiert ist, was diese Begriffe bedeuten?

21. Gemäß Artikel 1 des Vorschlags dient das ETIAS der Feststellung, ob mit der Anwesenheit eines von der Visumpflicht befreiten Reisenden im Hoheitsgebiet der Mitgliedstaaten ein Risiko irregulärer Migration oder ein Risiko für die Sicherheit oder die öffentliche Gesundheit verbunden ist. Der EDSB weist darauf hin, dass der Vorschlag das Risiko für die öffentliche Gesundheit durch eine Aufzählung spezifischer Kategorien von Krankheiten definiert[16], aber Risiken für die Sicherheit oder durch irreguläre Migration nicht definiert.

22. (Ein)Wanderung wird üblicherweise binär als entweder legal (regulär) oder illegal (irregulär) definiert. In der Praxis kann jedoch irreguläre Migration eine breite Palette von Verstößen gegen Einwanderungs- und andere Gesetze beinhalten; als Beispiele seien genannt die Einreise in einen Mitgliedstaat ohne die erforderliche Genehmigung oder die erforderlichen Dokumente, die Überschreitung der zulässigen Aufenthaltsdauer bei einer

Reise ohne Visum, das Untertauchen während des Asylverfahrens oder eine unterbleibende Ausreise aus einem Aufnahmemitgliedstaat nach einer abschlägigen Entscheidung.

23. Der EDSB hält fest, dass der Vorschlag nicht klar die Kategorien von Verstößen gegen Einwanderungs- (und andere) Gesetze aufführt, die ein Risiko irreguläre Migration darstellen können. Er entnimmt verschiedenen Bestimmungen des Vorschlags, dass eine Überschreitung der zulässigen Aufenthaltsdauer oder die Tatsache, dass gegen eine Person eine Rückführungsentscheidung ergangen ist, – unter anderem – Elemente sind, die bei der Bewertung des Risikos irregulärer Migration herangezogen werden. Der EDSB empfiehlt, genauer zu bedenken, welche Verstöße gegen (Ein)Wanderungsgesetze berücksichtigt werden sollten. Die Schwere des Verstoßes ist eine andere, je nachdem, ob ein Drittstaatsangehöriger mit falschen Dokumenten in einen Mitgliedstaat eingereist ist oder ob er für einige Tage seinen zulässigen Aufenthalt überzogen hat.

24. Bezüglich der Risiken für die Sicherheit stellt der EDSB fest, dass sie im Vorschlag ebenfalls nicht definiert sind. Ganz grundlegend bedeutet Sicherheit die Aufrechterhaltung von öffentlicher Ordnung und Sicherheit. Unter diesen Begriff fällt eine Fülle an Situationen, von Vandalismus bis zu terroristischen Handlungen. Auch wenn es im Vorschlag nicht deutlich zum Ausdruck kommt, besteht nach Ansicht des EDSB ein Kernelement der Bewertung eines Risikos für die Sicherheit in der Frage, ob der Drittstaatsangehörige einer Straftat verdächtigt wird oder wegen einer oder mehrerer Straftaten strafrechtlich verurteilt worden ist. Wie bei Einwanderungsrisiken sollten auch bei der Bestimmung von Risiken für die Sicherheit nur schwere Straftaten berücksichtigt werden.

25. **Der EDSB empfiehlt die Aufnahme einer Definition von Risiken durch irreguläre Migration und von Risiken für die Sicherheit in den Vorschlag. In der Definition des Risikos irregulärer Migration sollten die Kategorien von schweren Verstößen gegen Einwanderungsgesetze spezifiziert werden (z. B. durch Festlegung einer Schwelle für die Schwere des Verstoßes), die ein Risiko irregulärer Migration darstellen können. Mit Blick auf die Definition von Risiken für die Sicherheit empfiehlt der EDSB, zu überlegen, welche schweren Straftaten abgedeckt werden sollen, und dabei auch die in Artikel 3 Absatz 1 Buchstabe m des Vorschlags definierten heranzuziehen.**

3. ETIAS-Überprüfungsregeln als Profiling-Instrument

Profiling mit Hilfe des ETIAS

26. Artikel 28 Absatz 1 des Vorschlags sieht vor, dass ETIAS-Antragsdatensätze mit den ETIAS-Überprüfungsregeln abgeglichen werden, die definiert sind als *„ein Algorithmus, der den Abgleich zwischen den in einem Antragsdatensatz des ETIAS-Zentralsystems gespeicherten Daten und spezifischen Risikoindikatoren ermöglicht, die auf das Risiko der irregulären Migration oder Risiken für die Sicherheit und die öffentliche Gesundheit hindeuten“.*

27. In Artikel 28 Absatz 2 sind die Arten von Daten aufgeführt, die bei der Bestimmung des Risikos der irregulären Migration und des Risikos für die Sicherheit und die öffentliche Gesundheit herangezogen werden (also von den Mitgliedstaaten bereitgestellte Statistiken und Informationen), während Artikel 28 Absatz 4 eine Liste von Daten enthält, auf deren

Grundlage die ETIAS-Zentralstelle die spezifischen Risikoindikatoren festlegt. Die ETIAS-Zentralstelle ist für die Festlegung und Anpassung dieser spezifischen Risikoindikatoren nach Anhörung des ETIAS-Überprüfungsausschusses zuständig, der aus Vertretern von Europol und der einzelnen nationalen ETIAS-Stellen besteht (Artikel 28 Absatz 5). Artikel 28 besagt ferner, dass der Algorithmus im ETIAS-Zentralsystem gespeichert wird und dass die Kommission delegierte Rechtsakte zur näheren Spezifizierung des Risikos der irregulären Migration sowie der Risiken für die Sicherheit und die öffentliche Gesundheit erlassen wird. Dessen ungeachtet ist in Anbetracht der vorstehenden Ausführungen des EDSB eine vorherige Spezifizierung der genauen Bedeutung dieser Risiken erforderlich.[17]

28. Der EDSB geht davon aus, dass das Ziel der ETIAS-Überprüfungsregeln darin besteht, ein Instrument zu schaffen, dass ein automatisches Aussortieren von von der Visumpflicht befreiten Drittstaatsangehörigen ermöglicht, die im Verdacht stehen, ein Risiko der irregulären Migration oder ein Risiko für die Sicherheit oder die öffentliche Gesundheit darzustellen. Dieses Instrument dürfte für solche Personen nachteilige Folgen haben, denn letztendliches Ziel ist es, ihre Einreise in das Hoheitsgebiet der Mitgliedstaaten zu verhindern. **Im Sinne von Klarheit und Transparenz sollte die in Artikel 28 vorgeschlagene Technik der Datenverarbeitung, die ganz klar ein Profiling ist, auch ausdrücklich so genannt werden, damit alle für eine solche Verarbeitung benötigten Garantien hergestellt werden können.**

Folgenabschätzung für das Profiling

29. Profiling wirft genau wie jede andere Form der auf natürliche Personen angewandten computergestützten Datenauswertung, sofern es in natürliche Personen berührenden Entscheidungsprozessen angewandt wird, schwerwiegende technische, rechtliche und ethische Fragen auf. Ein Hauptproblem beim Profiling liegt darin, dass es unweigerlich mit einem hohen Grad an Verallgemeinerung und Ungewissheit einhergeht, und zwar sowohl was die Richtigkeit des vorhergesagten Verhaltens als auch die Genauigkeit der Zuweisung von Korrelationen ermittelter Muster zu bestimmten Merkmalen der Personen angeht. Des Weiteren erfordert die Beurteilung von Personen aus dem Blickwinkel eines geschaffenen Profils nicht nur die vorherige Zuweisung der Person zu einer Kategorie, sondern kann auch zu einer ungerechten oder voreingenommenen Behandlung bestimmter Kategorien oder Gruppen von Menschen führen.[18]

30. Daher stellt sich der EDSB besorgt die Frage, ob die Verwendung der ETIAS-Überprüfungsregeln in vollem Einklang mit den in der Charta verankerten Grundrechten und hier vor allem mit dem Recht auf Privatsphäre, Datenschutz und Nichtdiskriminierung stehen wird. **Der EDSB empfiehlt, die vorgeschlagenen ETIAS-Überprüfungsregeln zuvor einer umfassenden Bewertung ihrer Auswirkung auf Grundrechte zu unterziehen, bei der auch die Notwendigkeit und Verhältnismäßigkeit des Einsatzes eines solchen Instruments geprüft werden kann.**

Notwendigkeit von Profiling-Instrumenten

31. Der ETIAS-Vorschlag sieht jedoch nicht nur vor, dass jeder Antrag mit den ETIAS-Überprüfungsregeln abgeglichen wird, sondern auch, dass jeder in das ETIAS-Zentralsystem eingegebene Antrag zudem automatisch

- mit Informationen in anderen IT-Systemen der EU abgeglichen wird, die in Artikel 18 Absatz 2 aufgelistet sind, und
- mit bestimmten Werten (z. B. einer Telefonnummer oder einer IP-Adresse) auf einer nach Artikel 29 erstellten ETIAS-Überwachungsliste abgeglichen wird.

32. Während die Methode der Überprüfungsregeln auf einer Datenanalyse beruht und Profiling darstellt, beruhen diese beiden Methoden auf einem Vergleich von ETIAS-Daten mit in EU-Datenbanken gespeicherten oder in der Überwachungsliste für die Suche nach potenziellen Übereinstimmungen („Treffern“) zusammengestellten Informationen. In anderen IT-Systemen und der Überwachungsliste gespeicherte Daten sollten zuverlässiger sein als eine Überwachung mit Hilfe eines intransparenten Profils, das von einem Algorithmus erstellt wurde. Der EDSB fordert daher den Gesetzgeber auf, sich über die Notwendigkeit der Verwendung von Überprüfungsregeln für die Zwecke des ETIAS Gedanken zu machen, zumal der Vorschlag noch andere Instrumente für eine Prüfung der Frage bereithält, ob die Anwesenheit des Antragstellers im Hoheitsgebiet der Mitgliedstaaten ein Risiko der irregulären Migration oder ein Risiko für die Sicherheit oder die öffentliche Gesundheit darstellen würde.

33. **Der EDSB verlangt überzeugende Beweise dafür, dass es erforderlich ist, für die Zwecke des ETIAS Profiling-Instrumente einzusetzen, und, *quod non*, ermutigt den Gesetzgeber, zu überdenken, inwieweit der Einsatz des Profiling im Hinblick auf die angestrebten Ziele erforderlich ist.**

Verhältnismäßigkeit

34. Sofern sich der Einsatz von Profiling-Instrumenten als erforderlich erweist, sollte er verhältnismäßig sein. Der EDSB begrüßt den Hinweis der Kommission darauf, dass die Risikoindikatoren zielgerichtet und verhältnismäßig sein werden. Der EDSB fragt sich jedoch, ob der Vorschlag Garantien bietet, damit dieses Ziel erreicht wird und ein hinreichendes Maß an Schutz der Grundrechte gewährleistet ist.

35. Der Vorschlag sieht die Prüfung der Anträge aller von der Visumpflicht befreiten Drittstaatsangehörigen nach den ETIAS-Überprüfungsregeln vor[19], obwohl nur wenige von ihnen wohl tatsächlich ein bestimmtes Risiko darstellen und ihnen daher die Reisegenehmigung verweigert wird. Dieser automatisierte und intransparente Umgang mit personenbezogenen Daten bedeutet an sich schon einen schweren Eingriff in die Grundrechte einer unbegrenzten Zahl von Antragstellern, die einem Profiling unterzogen werden; hier sollte mit Blick auf das erwartete Ergebnis eines solchen Instruments eine Abwägung vorgenommen werden.

36. Zudem kann je nach der für die Entwicklung der spezifischen Risikoindikatoren verwendeten Methode, die sehr weit ausgelegt werden können, die Zahl der Personen, denen eine automatisierte Genehmigung aufgrund eines auf den Überprüfungsregeln beruhenden Treffers verweigert wird, relativ hoch sein, auch wenn diese Personen eigentlich kein Risiko darstellen.

37. Der EDSB begrüßt, dass bei einer Verweigerung der Antrag manuell von den nationalen ETIAS-Stellen weiter bearbeitet wird (Artikel 22). Die Verweigerung einer automatisierten Genehmigung ist jedoch eine Entscheidung, die den Antragsteller erheblich beeinträchtigen kann. In Anbetracht des Mangels an Transparenz des Verfahrens der Profilerstellung sind

Zweifel an der Wirksamkeit der manuellen Bearbeitung von Anträgen durch die ETIAS-Zentralstelle oder die nationalen ETIAS-Stellen erlaubt. Wie könnte eine wirklich gründliche Prüfung der aufgedeckten potenziellen Risiken gewährleistet sein, wenn die Mitarbeiter dieser Stellen selber die Gründe für die Verweigerung der Genehmigungen für die Reisenden nicht kennen oder nicht verstehen? Der EDSB kann in dem Vorschlag keinerlei Instrument erkennen, das der ETIAS-Zentralstelle oder nationalen ETIAS-Stellen erlauben würde, die auf den ETIAS-Überprüfungsregeln basierenden Treffer im Einzelnen zu bewerten.

38. Ähnliche Zweifel hegt der EDSB bezüglich der Wirksamkeit des Rechts von Antragstellern, Rechtsmittel einzulegen, wenn die Genehmigung nach einem Abgleich mit einem Profil verweigert wird. Damit einem Antragsteller wirklich ein Rechtsmittel an die Hand gegeben wird, müsste der für dieses Verfahren zuständige Mitgliedstaat in der Lage sein, die hinter der Erkennung von Risiken stehenden Gründe zu kennen und zu verstehen. Auch der Antragsteller, dem die Genehmigung verweigert wurde, müsste die Entscheidung verstehen, damit er Gelegenheit hat, sie von einer Beschwerdeinstanz verwerfen zu lassen.

Risiko der Diskriminierung

39. Der Vorschlag verbietet die Festlegung der spezifischen Risikoindikatoren auf der Grundlage der rassischen oder ethnischen Herkunft einer Person, ihrer politischen Meinungen, religiösen und weltanschaulichen Überzeugungen, ihrer Mitgliedschaft in einer Gewerkschaft, ihres Sexuallebens oder ihrer sexuellen Orientierung. Damit ist jedoch das Risiko einer Diskriminierung aufgrund solcher Kriterien nicht völlig ausgeschlossen. Gemäß Artikel 28 Absatz 4 gehören zu den Daten, die für die Festlegung der spezifischen Risikoindikatoren verwendet werden, unter anderem die derzeitige Staatsangehörigkeit, das Land und der Ort des Wohnsitzes eines Antragstellers sowie das Geschlecht und die derzeitige berufliche Tätigkeit.

40. Der EDSB weist darauf hin, dass die Risikoindikatoren zwar nicht direkt unter Verwendung solcher Kriterien festgelegt werden, dass aber das Ergebnis ganz ähnlich ausfallen würde, wenn sie verwendet würden. Informationen wie Staatsangehörigkeit und Ort des Wohnsitzes lassen, zumal in Verbindung mit anderen Daten, gewisse Rückschlüsse auf die rassische oder ethnische Herkunft des Antragstellers zu. In ähnlicher Weise können die Risikoindikatoren nicht auf der Mitgliedschaft in einer Gewerkschaft beruhen, können aber anhand der Informationen über die derzeitige berufliche Tätigkeit festgelegt werden. Diese Arten von Informationen sind auf das Engste miteinander verknüpft, und daher würde ein Profiling auf dieser Grundlage das Risiko einer Diskriminierung nicht wirklich ausräumen.

41. Aus allen diesen Gründen **fordert der EDSB den Gesetzgeber auf, die Notwendigkeit und Verhältnismäßigkeit des Profiling in einer gründlichen Datenschutzfolgenabschätzung nachzuweisen.**

4. Gesundheitsdaten

42. Eine der Zielsetzungen des ETIAS besteht darin, vor der Ankunft eines von der Visumpflicht befreiten Drittstaatsangehörigen zu prüfen, ob er möglicherweise ein Risiko für die öffentliche Gesundheit darstellt. Zu diesem Zweck müssen Antragsteller auf eine Reisegenehmigung beim Ausfüllen ihres Antrags über ETIAS Hintergrundfragen zu ihrer

Gesundheit beantworten. Gemäß Artikel 15 Absatz 4 Buchstabe a wird jeder Antragsteller gefragt, ob er eine Krankheit mit epidemiologischem Potenzial im Sinne der Internationalen Gesundheitsvorschriften der Internationalen Gesundheitsorganisation oder sonstige übertragbare, durch Infektionserreger oder Parasiten verursachte Krankheiten hat. Inhalt und Format dieser Fragen sind später von der Kommission in delegierten Rechtsakten zu bestimmen. Die einzigen für Zwecke der öffentlichen Gesundheit relevanten im ETIAS gespeicherten Fragen sind die mit „ja“ oder „nein“ zu beantwortenden Hintergrundfragen zur Gesundheit. Eine einzige bejahte Hintergrundfrage würde genügen, um eine manuelle Nachbearbeitung des Antrags auszulösen und vom Antragsteller weitere Informationen zu verlangen.

43. Gesundheitsbezogene Daten sind besonders sensible Daten, die Anspruch auf ein höheres Schutzniveau haben.[20]

44. Der EDSB begrüßt, dass die Abfrage von Gesundheitsdaten im ETIAS im Vorschlag insofern eingeschränkt wird, als sie für Strafverfolgungszwecke weder durch nationale Gefahrenabwehr- und Strafverfolgungsbehörden (Artikel 45 Absatz 2) noch durch Europol (Artikel 25 Absatz 3) erlaubt ist. Der EDSB stellt sich jedoch die Frage, welchen Mehrwert die Erhebung und Verarbeitung von Gesundheitsdaten über das ETIAS für das Ziel des Schutzes der öffentlichen Gesundheit in der EU erbringt, wie es in den Zielen des Vorschlags (Artikel 1 und 4) formuliert ist.

45. Gesundheitsdaten werden direkt beim Reisenden erhoben, ohne dass irgendeine Möglichkeit besteht, die Richtigkeit dieser Daten zu überprüfen. Selbst wenn der Antragsteller die Fragen nach seiner Gesundheit wahrheitsgemäß beantwortet hat, wäre die ETIAS-Genehmigung für fünf Jahre und für mehrere Reisen gültig, und in einem solchen Zeitraum kann sich der Gesundheitszustand einer Person durchaus verändern, und der Antragsteller hat dann keinerlei Möglichkeit, die in dem Online-Antragsformular eingereichten Angaben zu ändern. Damit wären die gespeicherten Gesundheitsdaten überholt und für Zwecke der öffentlichen Gesundheit irrelevant.

46. Hierzu besagt die Machbarkeitsstudie von 2016, dass zwar Risiken für die öffentliche Gesundheit (z. B. die Ausrottung der Tuberkulose) kürzlich zu einer Priorität der EU gemacht wurden, dass aber nur ein begrenzter Zusammenhang zwischen dem Erreichen dieses Ziels und der Erhebung von Gesundheitsdaten bei allen von der Visumpflicht befreiten Drittstaatsangehörigen besteht.[21] In der Studie heißt es hierzu erläuternd, dass die von diesen Risiken betroffenen Länder diejenigen sind, mit denen die EU erst dabei ist, Abkommen über Visa-Erleichterungen auszuhandeln. Dies veranlasst den EDSB, die Relevanz und Effizienz der derzeit vorgeschlagenen Verwendung des ETIAS als Beitrag zum Schutz der öffentlichen Gesundheit in Frage zu stellen.

47. Gemäß Erwägungsgrund 48 des Vorschlags soll Interoperabilität zwischen dem ETIAS und bestehenden Systemen wie beispielsweise SIS, VIS oder ECRIS bestehen, damit das Risiko für die Sicherheit oder die öffentliche Sicherheit oder das Risiko der irregulären Migration, das möglicherweise von einem Reisenden ausgeht, bewertet werden kann. Allerdings befasst sich keines dieser Systeme mit gesundheitlichen Aspekten, weshalb sie für die die öffentliche Gesundheit betreffenden Zwecke des ETIAS irrelevant sind.

48. Der EDSB bezweifelt, dass eine Verarbeitung dieser besonders sensiblen Datenkategorie in so großem Maßstab und über diesen Zeitraum den Vorgaben von Artikel 52 Absatz 1

der Charta genügt und folglich als erforderlich und verhältnismäßig betrachtet werden kann.

49. **Der EDSB stellt die Relevanz der im Vorschlag vorgesehenen Erhebung und Verarbeitung von Gesundheitsdaten in Frage, weil es ihnen an Belastbarkeit mangelt und weil aufgrund der nur schwachen Verbindung zwischen Risiken für die Gesundheit und von der Visumpflicht befreiten Reisenden keine Notwendigkeit hierfür besteht.**

5. Zugriff für Gefahrenabwehr- und Strafverfolgungsbehörden

50. Der Vorschlag sieht vor, dass von Anfang an nationale Gefahrenabwehr- und Strafverfolgungsbehörden und Europol zum Zwecke der Verhütung, Aufdeckung und Untersuchung terroristischer oder sonstiger schwerer Straftaten Zugriff auf das ETIAS-Zentralsystem haben (Artikel 1 Absatz 2).

51. Die Gewährung des Zugriffs auf ETIAS für Strafverfolgungszwecke würde zu einem allgemeinen Trend passen, der in der EU in den vergangenen Jahre zu beobachten war, und bei dem diesen Behörden Zugang zu IT-Großsystemen für Grenzen und Migration gewährt wird, ebenso zu Eurodac und VIS und dem vorgeschlagenen EES und dem vorgeschlagenen ECRIS.[22] Der Zugriff auf bestehende und künftige EU-Datenbanken für Gefahrenabwehr- und Strafverfolgungsbehörden sollte jedoch nicht zum Prinzip erhoben werden, sondern vielmehr nur in begrenzten Fällen gestattet werden, wenn Notwendigkeit und Verhältnismäßigkeit des Zugriffs umfassend begründet und nachgewiesen sind.

52. Nach Auffassung des EDSB sollte ein Zugriff zu ETIAS für Strafverfolgungszwecke im Vorschlag nur unter der Bedingung vorgesehen werden, dass ein solcher Zugriff nachweislich erforderlich und verhältnismäßig ist.

53. In der Begründung führt die Kommission aus, dass es *„unerlässlich ist, dass die zuständigen Gefahrenabwehr- und Strafverfolgungsbehörden Zugang zu relevanten und klar definierten Informationen im ETIAS haben, wenn dies für die Verhütung, Aufdeckung und Untersuchung terroristischer oder sonstiger schwerer Straftaten erforderlich ist“*.[23]

54. Die Kommission erwähnt allerdings nicht das künftige EES, das Informationen über alle (visumpflichtigen und von der Visumpflicht befreiten) Drittstaatsangehörigen enthält, die in den Schengen-Raum einreisen, und zu dem dann auch Gefahrenabwehr- und Strafverfolgungsbehörden Zugang hätten. Die im EES gespeicherten Datensätze würden große Ähnlichkeit mit den Datensätzen des VIS aufweisen (ausgenommen sind Daten, die mit den Visa direkt zu tun haben, z. B. die Visummarken)[24] und diese Informationen mit Einträgen zu Ein- und Ausreisen aller Reisenden ergänzen. Das EES wäre also in der Lage, Gefahrenabwehr- und Strafverfolgungsbehörden mindestens die gleichen Informationen über von der Visumpflicht befreite Drittstaatsangehörige zu bieten wie sie das VIS über visumpflichtige Drittstaatsangehörige bereithält. Die EU-PNR werden ebenfalls für Gefahrenabwehr- und Strafverfolgungsbehörden sowie Europol zugänglich sein und nähere Informationen über alle Flugpassagiere enthalten. ob nun mit oder ohne Visum.

55. Des Weiteren spricht die Kommission vom VIS als einem Beispiel für ein System, bei dem sich der Zugang für Strafverfolgungszwecke als zweckmäßig erwiesen hat. Als Beleg für

diese Aussage führt die Kommission aus: *„Der Zugriff auf die im Visa-Informationssystem (VIS) gespeicherten Daten zu Gefahrenabwehr- und Strafverfolgungszwecken hat sich bereits insofern als zweckmäßig erwiesen, als er dazu beigetragen hat, dass Ermittler in Fällen im Zusammenhang mit Menschenhandel, Terrorismus oder Drogenhandel erhebliche Fortschritte erzielt haben. Im Visa-Informationssystem sind allerdings keine Daten über von der Visumpflicht befreite Drittstaatsangehörige erfasst".*[25] Der EDSB weist darauf hin, dass im Datenschutz „zweckmäßig" nicht mit „erforderlich" gleichzusetzen ist.[26] Der von der Kommission Ende 2016 herausgegebene Bericht über die Evaluierung des VIS kommt zu dem Ergebnis, dass die Evaluierung des Zugriffs für Gefahrenabwehr- und Strafverfolgungsbehörden *„fragmentarisch und nicht eindeutig ausfällt".*[27]

56. Aufgrund der vorstehenden Erwägungen **verweist der EDSB in dieser Phase erneut auf die Notwendigkeit, überzeugende Beweise dafür vorzulegen, dass es erforderlich ist, ETIAS-Daten nationalen Gefahrenabwehr- und Strafverfolgungsbehörden und Europol zur Verfügung zu stellen. Der EDSB erinnert daran, dass Notwendigkeit und Verhältnismäßigkeit neuer Regelungen sowohl insgesamt, unter Berücksichtigung der bereits in der EU bestehenden IT-Großsysteme, als auch spezifisch, für jeden Einzelfall der Drittstaatsangehörigen zu bewerten sind, die rechtmäßig als Besucher in die EU einreisen**.[28]

IV. WEITERE EMPFEHLUNGEN

1. Datenqualität und Datenminimierung

57. Der EDSB erinnert daran, dass nach den Grundsätzen der Datenqualität und Datenminimierung personenbezogene Daten den Zwecken entsprechen müssen, für die sie erhoben werden, dafür erheblich sein müssen und auf das beschränkt sein müssen, das für die Zwecke, für die sie verarbeitet werden, erforderlich ist.

Relevanz der beim Antragsteller erhobenen Daten

58. In Artikel 15 des Vorschlags sind die Daten über den Antragsteller aufgelistet, die über das Antragsformular erhoben werden. In der Machbarkeitsstudie von 2016 zu ETIAS heißt es, dass im ETIAS-Antragsformular höchstens 26 Datenfelder auszufüllen sein werden und nicht 44 wie im Visumantrag.[29] Der EDSB hält jedoch fest, dass sich diese Zahlen kaum vergleichen lassen, weil laut Vorschlag alle erhobenen Daten (einschließlich Gesundheitsdaten und justizielle Daten) letztendlich im ETIAS zusammengeführt und gespeichert werden. Das heißt, dass in der Praxis im ETIAS mehr Daten als im VIS gespeichert werden.

59. Im Hinblick auf die einzelnen Arten von Daten, die im ETIAS erfasst werden, wiederholt der EDSB seine Forderung nach einer gründlichen Bewertung der Notwendigkeit für jede Art von Daten, die für die im Vorschlag vorgesehenen Zwecke verarbeitet werden. Der EDSB kann sich nicht der Ansicht anschließen, dass alle in Artikel 15 des Vorschlags aufgelisteten Arten von Daten für Zwecke der Sicherheit, der Migration oder der öffentlichen Gesundheit erforderlich sind. Daher besteht er auf entsprechenden

Begründungen, wobei besonders auf Daten wie beispielsweise die Bildung des Antragstellers, seine derzeitige berufliche Tätigkeit oder IP-Adresse zu achten ist.

60. Darüber hinaus stellt der EDSB fest, dass sich die von Europol erstellte Überwachungsliste zwar auf terroristische Straftaten und andere schwere Straftaten stützen wird (Artikel 29), in den vom Antragsteller zu beantwortenden Hintergrundfragen hingegen gefragt wird, ob er *jemals* wegen einer Straftat verurteilt worden ist (Artikel 15 Absatz 4). Nach Auffassung des EDSB dürfte eine Reihe von Straftaten (z. B. strafrechtlich zu ahndende Verkehrsvergehen) *a priori* für die Zwecke des ETIAS ohne Bedeutung sein. **Er empfiehlt, die im Zusammenhang mit Straftaten erhobenen Daten strikt auf terroristische Straftaten und schwere Straftaten im Sinne von Artikel 3 Absatz 1 Buchstaben l und m des Vorschlags zu beschränken** (also Straftaten, die den in Artikel 2 Absatz 2 des Rahmenbeschlusses 2002/584/JI des Rates aufgeführten Straftaten entsprechen oder gleichwertig sind, wenn die Straftaten mit einer freiheitsentziehenden Strafe oder Sicherungsmaßnahmen für eine Höchstdauer von mindestens drei Jahren nach dem nationalen Recht geahndet werden können).

Relevanz von Informationen aus anderen Systemen

61. Der Vorschlag richtet ein System ein, das mit anderen Systemen in den Bereichen Polizei, Justiz und Einwanderung interoperabel ist, damit in ETIAS erfasste Informationen mit den in diesen Systemen gespeicherten Informationen abgeglichen werden können. Der EDSB weist darauf hin, dass ein Abgleich von Daten im ETIAS mit allen in anderen Systemen gespeicherten Informationen für ETIAS-Zwecke möglicherweise unerheblich ist. So fragt sich der EDSB beispielsweise, inwiefern eine Ausschreibung im SIS nach Personen, die in einem Gerichtsverfahren als Zeugen auftreten sollen, eine Rolle bei der Bekämpfung von Risiken durch Einwanderung, für die Sicherheit oder die Gesundheit spielen kann. Ebenso gilt, dass nicht alle Straftaten, wegen denen der Antragsteller verurteilt worden ist und die im ECRIS gespeichert sind, für die Zwecke des ETIAS von Belang sind. **Der EDSB empfiehlt daher, genau festzulegen, welche Informationen in anderen Systemen für die Zwecke des ETIAS von Belang sind, und den Abgleich von ETIAS-Daten mit diesen Informationen strikt zu begrenzen.**

2. Datenspeicherung

62. Gemäß Artikel 47 Absatz 1 des Vorschlags wird jeder Antragsdatensatz im ETIAS-Zentralsystem gespeichert für

a) die Dauer der Gültigkeit der Reisegenehmigung;
b) fünf Jahre ab dem Datum des letzten im EES gespeicherten Einreisedatensatzes oder
c) fünf Jahre ab dem Datum der letzten Entscheidung über die Verweigerung, die Aufhebung oder die Annullierung der Reisegenehmigung.

63. Bei der Festlegung einer Datenspeicherfrist verlangen die EU-Datenschutzstandards einen möglichst kurzen Zeitraum, der sich nach dem Zweck richtet.[30]

Gültigkeitsdauer von fünf Jahren

64. Der EDSB nimmt die Gültigkeitsdauer von fünf Jahren für ETIAS-Genehmigungen zur Kenntnis (Artikel 30 Absatz 2). Die für ETIAS-Genehmigungen gewählte Gültigkeitsdauer wirkt sich unmittelbar auf die Frist für die Speicherung personenbezogener Daten im System aus.

65. In der Machbarkeitsstudie von 2016 heißt es hierzu: *„Für die Bequemlichkeit der Reisenden spricht ein möglichst langer Zeitraum“,* und weiter: *„Auch mit Blick auf die Kosten und den Arbeitsaufwand für die Antragsverwaltung wäre ein möglichst langer Zeitraum vorteilhaft“*.[31] Die Vorteile einer langen Gültigkeitsdauer würden allerdings durch die Tatsache zunichte gemacht, dass *„im Laufe der Zeit die nach der Antragstellung vorgenommene Risikobewertung an Relevanz verliert, weil sich die Lage der Person geändert haben kann“*. Die Studie kam zu dem Ergebnis, dass eine Gültigkeitsdauer zwischen zwei und fünf Jahren die beste Lösung wäre.

66. Der EDSB möchte wissen, warum sich die Kommission für den längsten der in der Machbarkeitsstudie von 2016 genannten Zeiträume entschieden hat, also für fünf Jahre, und nicht für einen kürzeren.

Fünf Jahre ab dem Datum des letzten Einreisedatensatzes

67. In den meisten Fällen[32] dürfte – im Einklang mit Artikel 47 Absatz 1 Buchstabe b – die Datenspeicherfrist für ETIAS in der Praxis der des EES entsprechen.

68. Laut Begründung des Vorschlags möchte die Kommission gewährleisten, *„dass der Einreisedatensatz und die entsprechende Reisegenehmigung gleich lange gespeichert werden“*[33], damit jede Einreise eines von der Visumpflicht befreiten Drittstaatsangehörigen in den Schengen-Raum mit einer Reisegenehmigung im ETIAS und einem entsprechenden Einreisedatensatz im EES verknüpft ist.

69. Nach Auffassung des EDSB rechtfertigt allein die Tatsache, dass die vorgeschlagene Speicherfrist für ETIAS-Daten an die Speicherfrist im EES – die wiederum an die Speicherfrist im VIS angeglichen ist – angeglichen wird und mit ihr übereinstimmt, diese Entscheidung nicht.[34]

Fünf Jahre ab einer Verweigerung, Aufhebung oder Annullierung

70. Der EDSB kann nicht nachvollziehen, warum ein Antrag auf eine verweigerte, aufgehobene oder annullierte ETIAS-Genehmigung, wie in Artikel 47 Absatz 1 Buchstabe c geregelt, fünf Jahre, also über einen langen Zeitraum, gespeichert werden soll.

Sonstige Anmerkungen

71. Sollte die Notwendigkeit der drei vorstehend genannten Aufbewahrungsfristen nachgewiesen werden, weist der EDSB auf Folgendes hin: Sollte es tatsächlich die Absicht der Kommission sein, eine Verknüpfung zwischen der Reisegenehmigung im ETIAS und dem entsprechenden Einreisedatensatz im EES herzustellen, geht aus Artikel 47 Absatz 1 Buchstabe b nicht klar hervor, dass die fünfjährige Speicherfrist für

ETIAS-Antragsdatensätze mit dem Datum des letzten Einreisedatensatz im EES auf der Grundlage der *entsprechenden* Reisegenehmigung beginnt.

72. Ferner fragt sich der EDSB nach dem Mehrwert, den die Aufbewahrung des Inhalts des gesamten Antragsdatensatzes über die Gültigkeitsdauer der Reisegenehmigung hinaus und für einen Zeitraum, der so lang ist wie der des entsprechenden Einreisedatensatzes, mit sich brächte. Für die Zwecke des EES würde es genügen, lediglich den Status des Antragsdatensatzes (also „erteilt" oder „verweigert") anzugeben und nicht den ganzen Antragsdatensatz zu speichern.

73. Unklar ist dem EDSB ferner, welchen Mehrwert die Speicherung der Antworten „ja" und „nein" auf die Hintergrundfragen für so lange Zeiträume brächte. Abgesehen von der Tatsache, dass ETIAS-Daten weniger belastbar sind, weil sie rein deklarativer Art sind und bei den Antragstellern erhoben werden, können sich die Antworten auf die gleichen Hintergrundfragen im Verlauf von fünf Jahren wirklich ändern.

74. **Der EDSB fordert den Gesetzgeber auf, eine bessere Begründung für die in Artikel 47 Absatz 1 Buchstaben a, b und c gewählten Speicherfristen vorzulegen, damit gewährleistet ist, dass die Speicherung von ETIAS-Daten auf das für die Zwecke des Systems unbedingt Notwendige beschränkt wird. Der EDSB empfiehlt ferner, für die verschiedenen Kategorien gespeicherter Daten unterschiedliche Fristen festzulegen.**

3. Interaktion mit anderen Informationssystemen

75. Der EDSB hält fest, dass ETIAS mit anderen Systemen in den Bereichen Polizei, Justiz und Einwanderung interoperabel sein soll. Der EDSB betont, dass jedes dieser Systeme für einen bestimmten Zweck eingerichtet wurde, der möglicherweise mit dem Zweck des ETIAS unvereinbar ist. Ein Beispiel: Der Zweck des Systems Eurodac besteht darin, bei der Bestimmung des Mitgliedstaats zu helfen, der für die Prüfung eines Antrags auf internationalen Schutz zuständig ist, und die Anwendung der Dublin-Verordnung zu erleichtern.[35] Es ist nicht darauf angelegt, bei der Ermittlung von Risiken durch Einwanderung zu helfen. Auch die noch nicht verabschiedeten Vorschläge zur Änderung der Rechtsgrundlage bestehender Systeme (also Eurodac, SIS II, ECRIS) oder zur Schaffung neuer Systeme (also EES) verfolgen einen spezifischen Zweck, der unter Umständen von den Zwecken des ETIAS abweicht. Der EDSB geht davon aus, dass das Ziel eines ECRIS, in dem strafrechtliche Verurteilungen von Drittstaatsangehörigen gespeichert sind, darin besteht, Richter und Staatsanwälte zu unterstützen und ihnen einfachen Zugriff auf Informationen über die Vorstrafen der betreffenden Personen zu verschaffen.

76. **Dem EDSB ist nichts von einer Prüfung der Vereinbarkeit der jeweiligen Ziele der im Vorschlag erwähnten Systeme mit den erklärten Zwecken des vorgeschlagenen ETIAS bekannt. Er weist nachdrücklich darauf hin, dass je nach den Ergebnissen einer solchen Prüfung möglicherweise Änderungen an den Rechtsgrundlagen der anderen Systeme sowie weitere Bedingungen erforderlich werden. Seiner Auffassung nach ist eine solche Prüfung unbedingt geboten, bevor erwogen wird, den Zugriff auf in anderen Systemen erhobene und gespeicherte Daten und deren Verwendung zu gewähren.**

4. Rechte betroffener Personen und Rechtsbehelfe

77. Der EDSB begrüßt die Möglichkeit für betroffene Personen, Rechtsmittel gegen die Verweigerung einer Reisegenehmigung einzulegen, die in dem Mitgliedstaat, der über den Antrag entschieden hat, im Einklang mit dem nationalen Recht dieses Mitgliedstaats einzulegen sind (Artikel 31).

78. Nach Ansicht des EDSB sind jedoch einige der in Artikel 31 Absatz 1 aufgeführten Gründe für eine Verweigerung nicht eindeutig genug; dort heißt es z. B. wenn der Antragsteller *„b) ein Risiko irregulärer Migration darstellt“* oder *„c) ein Risiko für die Sicherheit darstellt“*. Der Antragsteller sollte hinreichend klare Angaben zu dem/den Grund/Gründen für die Verweigerung erhalten, damit er wirksam Rechtsbehelf einlegen und die Gründe für die Verweigerung anfechten kann. **Der EDSB empfiehlt, die den Antragstellern im Fall einer Verweigerung der Genehmigung bereitzustellenden Informationen näher zu spezifizieren, vor allem dann, wenn die Verweigerung auf einen Treffer in einem anderen System zurückgeht.** Auf diese Weise würde der Antragsteller auch erfahren, für welches System er sein Recht auf Auskunft über die ihn in diesem System betreffenden personenbezogenen Daten und möglicherweise sein Recht auf Berichtigung und/oder Löschung ausüben sollte, falls ein Fehler festgestellt wurde oder seine Daten auf unrechtmäßige Weise verarbeitet wurden.

79. Gleiches sollte gelten für den Fall, dass die ETIAS-Genehmigung ursprünglich erteilt, später aber annulliert oder aufgehoben wurde (Artikel 34 und 35).

5. Unabhängige Überprüfung der Zugriffsbedingungen

80. Sollte die Notwendigkeit und Verhältnismäßigkeit des Einsatzes von ETIAS als Instrument der Gefahrenabwehr und Strafverfolgung nachgewiesen sein, müssten die Bedingungen für einen solchen Zugriff streng geregelt sein. Der EDSB nimmt die Bedingungen für einen solchen Zugriff auf ETIAS-Daten in Artikel 45 des Vorschlags zur Kenntnis. Der EDSB begrüßt Erwägungsgrund 35 des Vorschlags, in dem geregelt ist, dass ein Antrag von Gefahrenabwehr- und Strafverfolgungsbehörden *„zuvor von einem Gericht oder von einer Behörde geprüft wird, die Garantien für ihre völlige Unabhängigkeit und Unparteilichkeit bietet“*. **Nach Auffassung des EDSB kommt einer solchen Vorabprüfung erhebliche Bedeutung zu, und er empfiehlt, sie in Artikel 45 ausdrücklich zu erwähnen.**

81. Seiner Ansicht nach führt Artikel 44 Absatz 2 zu einer gewissen Unklarheit. Einerseits müssen nach Artikel 44 Absatz 2 die Mitgliedstaaten dafür sorgen, dass Anträge von Gefahrenabwehr- und Strafverfolgungsbehörden auf Abfrage entsprechend dem nationalen Recht und dem Verfahrensrecht effizient und zeitnah darauf überprüft werden, ob die Bedingungen von Artikel 45 erfüllt sind. In Artikel 44 Absatz 3 heißt es dann, dass die zentrale Zugangsstelle, sofern die Bedingungen erfüllt sind, die Anträge bearbeitet und die Daten übermittelt. Andererseits besagt Erwägungsgrund 37 des Vorschlags: „Die nationalen ETIAS-Stellen sollten als zentrale Anlaufstellen fungieren und prüfen, ob die Bedingungen für die Beantragung des Zugangs zum ETIAS-Zentralsystem im konkreten Einzelfall erfüllt sind“.

82. In Verbindung mit Erwägungsgrund 35 schlägt Artikel 44 Absatz 2 vor, dass noch ein weiterer Akteur tätig wird, nämlich ein Gericht oder eine [andere] unabhängige und unparteische Behörde, die überprüft, ob die Bedingungen für die Übermittlung des Antrags an die zentrale Zugangsstelle und die Bearbeitung des Antrags durch die zentrale Zugangsstelle erfüllt sind, wenn die Bedingungen von Artikel 45 erfüllt sind. Erwägungsgrund 37 hingegen sieht diese Funktion für die nationalen ETIAS-Stellen vor, die als zentrale Anlaufstellen fungieren. **Der EDSB empfiehlt daher, das Verfahren für den Zugriff klarzustellen.**

6. Verteilung von Rollen und Verantwortlichkeiten

83. Im Datenschutzrecht bezeichnet der Begriff „für die Verarbeitung Verantwortlicher" die Stelle, die die Zwecke und Mittel der Verarbeitung festlegt. Sind die Zwecke und Mittel der Verarbeitung gesetzlich festgelegt, kann das Gesetz auch die (Kriterien für die) Benennung des für die Verarbeitung Verantwortlichen enthalten.

84. Die Verteilung der Rollen und Verantwortlichkeiten im vorgeschlagenen ETIAS ist recht komplex, und der EDSB weiß die Bemühungen um eine klare Abgrenzung im Vorschlag zu würdigen. Für die Verarbeitung Verantwortlicher wird die Europäische Agentur für die Grenz- und Küstenwache (EAGK) sein. während eu-LISA der Auftragsverarbeiter ist (Artikel 50 und 51). Ferner sieht der Vorschlag vor, dass eu-LISA für die Entwicklung des gesamten Systems zuständig und für dessen Sicherheit verantwortlich sein wird. Dem Vorschlag ist zu entnehmen, dass eu-LISA diese Aufgaben ohne Beteiligung der EAGK wahrnehmen wird.

85. Zwar sind im Vorschlag die Zwecke (und bis zu einem gewissen Maß auch die Mittel) von ETIAS definiert, doch muss der für die Verarbeitung Verantwortliche Rechenschaft über das Treffen technischer und organisatorischer Maßnahmen ablegen, die geeignet sind, zu gewährleisten, dass die Verarbeitung im Einklang mit den Datenschutzvorschriften erfolgt, und sollte er nachweisen können, dass dies der Fall ist (z. B. durch Vorlage von Beweisen über ein ordnungsgemäßes Management der Informationssicherheit).

86. Mit der im Vorschlag vorgesehenen Rollenverteilung könnte sich die EAGK in der Lage wiederfinden, (als für die Verarbeitung Verantwortlicher) für Aspekte zur Rechenschaft gezogen zu werden, auf die sie keinen Einfluss hat (z. B. wie eu-LISA die Informationssicherheit in ETIAS managt), da sie ausschließlich eu-LISA zugewiesen wurden.

87. **Der EDSB empfiehlt eine präzisere Beschreibung der Rollenverteilung auf EAGK und eu-LISA und gegebenenfalls ihre Ernennung zu gemeinsam für die Verarbeitung Verantwortlichen.**[36]

7. Vorherige Überprüfung von Zugangsanträgen von Europol durch den EDSB

88. Unter bestimmten Voraussetzungen sollen ETIAS-Daten für Gefahrenabwehr- und Strafverfolgungsbehörden zugänglich sein. Nach Artikel 44 Absatz 2 des Vorschlags sorgen die Mitgliedstaaten dafür, *„dass ein Antrag auf Abfrage entsprechend [ihrem] nationalen Recht und dem Verfahrensrecht unabhängig, effizient und zeitnah überprüft*

wird". In der Begründung wird erläutert, dass er durch *„ein Gericht oder eine Behörde geprüft wird, die Garantien für ihre völlige Unabhängigkeit und Unparteilichkeit bietet"*.[37]

89. Gemäß Artikel 46 des Vorschlags hat Europol Zugriff auf ETIAS-Daten unter ähnlichen Bedingungen wie nationale Gefahrenabwehr- und Strafverfolgungsbehörden (z. B. wenn die Abfrage im Einzelfall erforderlich ist, wenn die Abfrage anderer Datenbanken keine Ergebnisse gezeitigt hat usw.). Ähnlich wie der Zugriff für nationale Gefahrenabwehr- und Strafverfolgungsbehörden unterliegt auch der Zugriff für Europol einer (im Vorschlag dem EDSB übertragenen) vorherigen Überprüfung *„gegebenenfalls gemäß dem Verfahren nach Artikel 44 der Verordnung (EU) 2016/794"*.

90. Am wichtigsten ist der Hinweis, dass der EDSB von seiner Funktion her kein Äquivalent zu den Behörden ist, die den Zugriff auf nationaler Ebene genehmigen. Auf der nationalen Ebene sind die überprüfenden Behörden Gerichte oder ähnliche Behörden (je nach Rechtsordnung Untersuchungsrichter, Staatsanwälte usw.). Es trifft zu, dass es derzeit auf europäischer Ebene keine eindeutiges Äquivalent gibt, denn der Europäische Gerichtshof spielt keine Rolle bei der Genehmigung einzelner Ermittlungsmaßnahmen, und die Europäische Staatsanwaltschaft wurde noch nicht errichtet (und dürfte einen anderen Aufgabenbereich als Europol haben). Aufgabe des EDSB ist es, die Einhaltung der Datenschutzvorschriften zu überwachen und zu kontrollieren, und nicht, einzelne Ermittlungsaktivitäten zu genehmigen. Der EDSB hat empfohlen, dass überprüfende Behörden von der Behörde unabhängig sein sollten, deren Tätigkeiten sie überprüfen[38], daraus folgt jedoch nicht, dass der EDSB die überprüfende Behörde sein sollte.

91. Zudem gilt nach dem Verfahren von Artikel 44 der Verordnung (EU) 2016/794[39] über Europol, dass in Fällen, die Daten aus mehreren Mitgliedstaaten betreffen, der EDSB die Datenschutzbehörde des Mitgliedstaats konsultiert, bevor er eine Entscheidung trifft. Im Fall einer aufgehobenen oder annullierten Genehmigung (Entscheidung einer nationalen ETIAS-Stelle) kann davon ausgegangen werden, dass die Daten unter diese Bestimmung fallen. In derartigen Konsultationen kann der EDSB der Datenschutzbehörde des Mitgliedstaats eine Antwortfrist zwischen einem und drei Monaten setzen.[40] In Fällen „besonderer Dringlichkeit"[41] kann der EDSB umgehend tätig werden und informiert die betreffende Datenschutzbehörde nachträglich und begründet die Dringlichkeit sowie die eingeleiteten Maßnahmen. Eine solche Situation sollte als Ausnahme und nicht als Standardverfahren angesehen werden. Zwar ist im Vorschlag nicht definiert, was unter einer *„effizienten und zeitnahen"* vorherigen Prüfung (Artikel 46 Absatz 3) zu verstehen ist, doch scheint der zeitliche Rahmen deutlich enger abgesteckt zu sein, als das Verfahren nach Artikel 44 der Verordnung (EU) 2016/794 liefern kann. Nach dem jetzigen Wortlaut könnte das Verfahren somit den EDSB in eine Lage bringen, in der er nach dem Gesetz nicht das liefern kann, was von ihm verlangt wird.

92. **Aus den vorstehend ausgeführten Gründen empfiehlt der EDSB, eine andere unabhängige Überprüfungsbehörde als den EDSB zu benennen.**

8. Überprüfung durch die ETIAS-Zentralstelle

93. Zwei Aspekte des ETIAS werden weder im Vorschlag noch in der Begründung detailliert genug beschrieben, nämlich zum einen die Art von Abfragen, die in anderen Informationssystemen durchgeführt werden sollen, und die Art, wie sie durchgeführt

werden, und zum anderen Art und Menge der in einem Treffer enthaltenen Informationen. Gemäß Artikel 3 Absatz 1 Buchstabe k des Vorschlags bedeutet *„Treffer" „eine Übereinstimmung, die anhand eines Abgleichs der in einem Antragsdatensatz des ETIAS-Zentralsystems erfassten personenbezogenen Daten mit den personenbezogenen Daten in einem Datensatz [...] in einem vom ETIAS-Zentralsystem abgefragten Informationssystem [...] festgestellt wird"*. Nach dieser Definition kann ein Treffer einfach als Boolesches Feld verstanden werden, in dem die einzig möglichen Werte *richtig* oder *falsch* sind. In der Frage, wie die Abfragen vorgenommen werden, geht der EDSB mit Blick auf Artikel 19 Absatz 3 davon aus, dass sie *keine eindeutigen* Antworten bezüglich der Identifizierung des Antragstellers ergeben.[42] Falls die Antworten auf Abfragen im Zusammenhang mit einem Antrag nicht eindeutig ausfallen, soll die ETIAS-Zentralstelle *„überprüfen können, ob die in dem Antragsdatensatz gespeicherten Daten den Daten in einem/einer der abgefragten Informationssysteme/Datenbanken [...] entsprechen"*.[43]

94. Wie kann nun aber die ETIAS-Zentralstelle diese Überprüfung vornehmen, wenn die einzigen der ETIAS-Zentralstelle vorliegenden Informationen der Antragsdatensatz und die Angabe Treffer/kein Treffer sind? Es gibt nur zwei Möglichkeiten: Ein *Treffer* enthält in Wirklichkeit mehr Informationen als die, die derzeit im Vorschlag genannt werden, und zeigt die in den mit ETIAS verbundenen Systemen enthaltenen Informationen den an einer Überprüfung beteiligten Stellen, also ETIAS-Zentralstelle und nationale ETIAS -Stellen (die eine Rechtsgrundlage für den Zugriff auf diese Art von Informationen haben oder auch nicht) an; oder die ETIAS -Zentralstelle und die nationalen ETIAS-Stellen haben Zugriff auf alle Informationssysteme, die ETIAS abfragen wird. Beide Szenarien erfordern eine Überarbeitung sowohl des ETIAS-Vorschlags als auch der Rechtstexte für alle die von ETIAS abgefragten Systeme.

95. **Der EDSB empfiehlt, klarzustellen, wie die Überprüfung durch die ETIAS-Zentralstelle vorgenommen werden kann. Wenn hier Klarheit besteht, sollte der Gesetzgeber alle erforderlichen Änderungen am Vorschlag vornehmen, damit a) der Zugriff der ETIAS-Zentralstelle zu den Informationen genau spezifiziert ist, die für die Überprüfung der Anträge erforderlich sind, und/oder b) die ETIAS-Zentralstelle nicht länger die Rolle hat, *nicht eindeutige* Anträge zu überprüfen.**

9. Architektur und Informationssicherheit

96. Da so viele verschiedene Stellen Zugriff auf die Daten haben und das ETIAS-Zentralsystem Zugang zu so vielen anderen hat, kommt der Koordinierung der Informationssicherheit allergrößte Bedeutung zu, denn jedes der beteiligten Informationssysteme oder jede beteiligte Stelle ist nur so sicher wie das schwächste Glied in der Kette. Eine hohe Informationssicherheit lässt sich jedoch nur durch eine gründliche Analyse der Risiken für die Informationssicherheit erreichen, denen das Informationssystem ausgesetzt ist. Selbst wenn man die im Vorschlag dargestellten Informationssicherheitsmaßnahmen als absolutes Minimum betrachten könnte, weist der EDSB doch nachdrücklich auf die Bedeutung eines angemessenen Managements der Risiken für die Informationssicherheit hin, wie es in Artikel 22 der Verordnung (EG) Nr. 45/2001 vorgegeben ist, der auch in Artikel 52 des Vorschlags erwähnt wird.

97. ETIAS würde eine grundlegende Veränderung der derzeitigen Architektur von IT-Großsystemen bedeuten, die von eu-LISA betreut und gemanagt werden: Eine

geschlossene Umgebung, zu der nur die Mitgliedstaaten und vielleicht einige andere Stellen der EU Zugang haben, öffnet eine Tür zum gesamten Internet.[44] Die Konsequenzen einer solchen Entscheidung für die Informationssicherheit sollten nicht unterschätzt werden, weshalb eine gründliche Analyse in Auftrag gegeben, durchgeführt und überprüft werden muss. Ferner haben bisher noch keine Systeme auf die Weise eine Infrastruktur geteilt, wie es für ETIAS und EES vorgeschlagen wird, und auch hier gilt, dass diese Entscheidung betreffend die technische Architektur wohl bedacht sein will und begleitender Dokumentation bedarf; ferner muss eu-LISA eine spezifische Analyse der Risiken jeder einzelnen Lösung ins Auge fassen und durchführen.

98. Der Vorschlag beschreibt zudem sehr detailliert die Architektur des Systems, beschränkt aber die technischen Optionen, für die man sich bei der Analyse und Festlegung der technischen Lösung(en) entscheiden kann. Die vorgeschlagene Verordnung sollte keine Vorgaben für irgendeine konkrete Entscheidung über die Architektur machen, sofern sie sich nicht auf andere Teile der Verordnung auswirkt, sondern sollte auf einen angemessenen Datenschutz und eine gründliche Sicherheitsanalyse zur Begleitung der Entwicklung des Systems achten.

99. Artikel 63 des Vorschlags schließlich beschreibt die Aufgaben im Bereich der Entwicklung und des operativen Managements für das ETIAS-System. Datenschutz und Datensicherheit werden hier jedoch nicht erwähnt. Ein neues System und jede größere Änderung eines bestehenden Systems (im vorliegenden Fall ist es nicht nur ein System, sondern EES, VIS, *die Europol-Daten*, SIS, Eurodac und ECRIS[45]) lässt sich professionell nur bewerkstelligen durch 1) Einhaltung eines angemessenen Sicherheitsprozesses, zu dem eine detaillierte Analyse der Risiken für die Informationssicherheit gehört, und 2) Einhaltung der Grundsätze des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen.

100. Ferner erteilt der Vorschlag der Kommission den Auftrag, *„detaillierte Bestimmungen [...] über Datenschutz- und Sicherheitsvorschriften [...] zu erlassen. Diese Durchführungsmaßnahmen werden nach dem Prüfverfahren gemäß Artikel 79 Absatz 2 erlassen“*, z. B. betreffend die öffentliche Website und die mobile App für Mobilgeräte[46], den Datenzugriff durch Beförderungsunternehmer zu Überprüfungszwecken[47] oder die Verwendung von Daten zur Erstellung von Berichten und Statistiken[48]. In allen diesen Fällen sollte der Vorschlag zwingend vorschreiben, dass Grundlage für diese *detaillierten Bestimmungen* über Datenschutz und -sicherheit das Risikomanagement der Informationssicherheit bzw. der Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen sind.

101. **Der EDSB empfiehlt, in Artikel 63 die Verpflichtung zur Durchführung und Fortführung einer Risikobewertung der Informationssicherheit und zur Wahrung der Grundsätze des Datenschutzes durch Technikgestaltung und datenschutzfreundliche Voreinstellungen hinzuzufügen.**

102. Im Hinblick auf die Artikel, in denen die Kommission mit der Annahme detaillierte Bestimmungen zum Datenschutz und zur Sicherheit beauftragt wird (Artikel 14, 59, 40 und 73) **empfiehlt der EDSB, dort jeweils auf die Notwendigkeit hinzuweisen, ein Risikomanagement für Informationssicherheit sowie Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen zu erwägen**.

103. **Des Weiteren empfiehlt der EDSB eine Änderung von Artikel 6 dahingehend, dass dort nur noch die Elemente aufgeführt werden, die für die vorgeschlagene Verordnung benötigt werden, und dass eu-LISA und den übrigen Interessenträgern die Gestaltung der endgültigen Architektur des ETIAS überlassen wird.**

104. Auch wenn in Artikel 50 des Vorschlags der EAGK die Rolle des für die Verarbeitung Verantwortlichen zugewiesen wird, wird ihr keinerlei Verantwortung für die Sicherheit der Verarbeitung übertragen. Ein für die Verarbeitung Verantwortlicher ist jedoch auch für die Sicherheit des Verarbeitungsvorgangs verantwortlich.[49] Selbst wenn eu-LISA[50] alle Sicherheitsanalysen und -maßnahmen durchführen sollte und größtenteils oder ganz für die Sicherheit des ETIAS zuständig ist, sollte die EAGK doch weiterhin für die durch die ETIAS-Zentralstelle erfolgende Verarbeitung personenbezogener Daten verantwortlich sein.

105. **Der EDSB empfiehlt, Artikel 52 und/oder Artikel 65 dahingehend abzuändern, dass die Verantwortung der EAGK für die Informationssicherheit anerkannt wird.**

10. Statistiken

106. Der EDSB sieht durchaus die Notwendigkeit für dazu befugte Mitarbeiter der zuständigen Behörden der Mitgliedstaaten, der Kommission, von eu-LISA und der ETIAS-Zentralstelle, Berichte und Statistiken zu den Daten im ETIAS zu erstellen. Anders als es in Artikel 73 des Vorschlags heißt, könnte allerdings die Menge der abrufbaren Daten eine Identifizierung einzelner Personen ermöglichen. So kann beispielsweise die Kombination von Staatsangehörigkeit, Geschlecht und Geburtsdatum eines Drittstaatsangehörigen durchaus zu einer Identifizierung führen.

107. **Der EDSB empfiehlt daher eine Umformulierung von Artikel 73, mit der eingeräumt wird, dass die in Artikel 73 Absatz 1 Buchstaben a bis i aufgelisteten Daten zu einer Identifizierung einzelner Personen führen können und daher ähnlich wie der Rest des ETIAS geschützt werden müssen.** Das bedeutet, dass eine ordnungsgemäße Risikobewertung der Informationssicherheit durchgeführt werden muss und angemessene Sicherheitsvorkehrungen getroffen werden müssen, bevor dieses weitere Zentralregister bereitgestellt wird.

108. Der EDSB warnt nachdrücklich davor, dass die derzeit für die Erstellung von Statistiken vorgeschlagene Lösung eine große Belastung für eu-LISA darstellt, denn sie müsste ein zweites Register pflegen und angemessen sichern, aber auch für den EDSB, denn er müsste die Aufsicht über dieses zweite Register übernehmen. Der EDSB würde eine Lösung bevorzugen, die kein weiteres Zentralregister erfordert, sondern eher von eu-LISA verlangt, Funktionalitäten zu entwickeln, die den Mitgliedstaaten, der Kommission, eu-LISA und der ETIAS-Zentralstelle die Möglichkeit gäben, die notwendigen Statistiken direkt aus dem ETIAS-Zentralsystem zu extrahieren, ohne dass ein weiteres Register erforderlich wäre.

109. Sollte jedoch ein anderes Register umgesetzt werden, könnte der Vorschlag im Einklang mit der ausdrücklichen Bereitschaft, anonyme Informationen zu verwenden, die Möglichkeit erkunden, eine den Datenschutz verstärkende Technologie wie Fernzugriff auf Daten (*Remote Data Access*) und *Differential Privacy* einzusetzen, damit

personenbezogene Daten verarbeitet werden können, ohne dass tatsächlich auf sie zugegriffen werden muss.

110. Anders als in anderen Verordnungen über IT-Großsysteme besteht schließlich nach Artikel 73 keine Verpflichtung zur Veröffentlichung der Jahresstatistiken.

11. Rolle des EDSB

111. Der EDSB ist die Datenschutzbehörde, die die Aufsicht sowohl über eu-LISA als auch die EAGK wahrnimmt.[51] Der EDSB ist zwar befugt, von den Organen, Einrichtungen und sonstigen Stellen der EU alle für die Wahrnehmung seiner Aufgaben erforderlichen Informationen zu erhalten[52], doch sollte das Verfahren gestrafft werden, indem der EDSB in die Liste der Empfänger der Berichte aufgenommen wird, die eu-LISA oder die ETIAS-Zentralstelle der Kommission, dem Rat oder dem Europäischen Parlament vorlegen[53].

112. Des Weiteren **empfiehlt der EDSB, in Artikel 57 eine Artikel 56 Absatz 2 ähnliche Bestimmung aufzunehmen, damit der EDSB die Ressourcen erhält, die er für eine ordnungsgemäße Kontrolle dieses neuen Systems benötigt.**

V. SCHLUSSFOLGERUNG

113. Der EDSB begrüßt die Aufmerksamkeit, die dem Datenschutz in dem Vorschlag über das ETIAS durchgehend geschenkt wird.

114. Der EDSB erkennt durchaus an, dass der Gesetzgeber bei der Beurteilung der Notwendigkeit und Verhältnismäßigkeit der vorgeschlagenen Maßnahmen eine wichtige Rolle spielt, weist aber darauf hin, dass diese beiden in der Charta verankerten hochrangigen rechtlichen Vorgaben vom Gerichtshof der Europäischen Union geprüft werden können und es Aufgabe des EDSB ist, sie zu schützen. Er unterstreicht, dass es aufgrund der fehlenden (Datenschutz-)Folgenabschätzung nicht möglich ist, die Notwendigkeit und Verhältnismäßigkeit des ETIAS in der derzeit vorgeschlagenen Form zu beurteilen.

115. Da der Vorschlag die Einrichtung eines weiteren Systems vorsieht, in dessen Rahmen erhebliche Mengen personenbezogener Daten von Drittstaatsangehörigen für Einwanderungs- und Sicherheitszwecke verarbeitet werden, rät der EDSB dem Gesetzgeber, eine Bestandsaufnahme aller auf EU-Ebene bestehenden Maßnahmen vorzunehmen, in deren Rahmen Daten für Migrations- und Sicherheitszwecke verarbeitet werden, und eine gründliche Analyse ihrer Zielsetzungen und ihrer Wirksamkeit durchzuführen.

116. In diesem Zusammenhang empfiehlt der EDSB, in den Vorschlag eine Definition von Risiken der irregulären Migration und Risiken für die Sicherheit aufzunehmen, um dem Grundsatz der Zweckbindung Genüge zu tun.

117. Zweifel hegt der EDSB auch in der Frage, ob die Anwendung der ETIAS-Überprüfungsregeln vollkommen in Einklang mit den in der Charta verankerten Grundrechten steht. Er empfiehlt, die vorgeschlagenen ETIAS-Überprüfungsregeln vorab einer umfassenden Prüfung ihrer Auswirkungen auf Grundrechte zu unterziehen. Des Weiteren fragt er sich, ob überzeugende Beweise für die Notwendigkeit der Verwendung von Profiling-Instrumenten für die Zwecke des ETIAS vorliegen, und, *quod non*, fordert er den Gesetzgeber auf, den Einsatz des Profiling zu überdenken.

118. Der EDSB stellt die Relevanz und Effizienz der im Vorschlag geplanten Erhebung und Verarbeitung von Gesundheitsdaten in Frage, weil es ihnen an Belastbarkeit mangelt. Fragen ergeben sich für ihn auch bezüglich der Notwendigkeit der Verarbeitung solcher Daten, weil zwischen Risiken für die Gesundheit und von der Visumpflicht befreiten Reisenden nur eine schwache Verbindung besteht.

119. Mit Blick auf den Zugriff auf ETIAS-Daten für Gefahrenabwehr- und Strafverfolgungsbehörden und Europol unterstreicht der EDSB, dass bis heute keine überzeugenden Beweise für die Notwendigkeit eines solchen Zugriffs vorliegen. Der EDSB erinnert daran, dass Notwendigkeit und Verhältnismäßigkeit neuer Regelungen sowohl insgesamt, unter Berücksichtigung der bereits in der EU bestehenden IT-Großsysteme, als auch spezifisch, für jeden Einzelfall der Drittstaatsangehörigen zu bewerten sind, die rechtmäßig als Besucher in die EU einreisen.

120. Neben den wichtigsten Bedenken, die vorstehend genannt wurden, betreffen die Empfehlungen des EDSB in der vorliegenden Stellungnahme folgende Aspekte des Vorschlags:
    - die Notwendigkeit und Verhältnismäßigkeit des erhobenen Datensatzes,
    - die gewählten Speicherfristen für die Daten,
    - die Interoperabilität des ETIAS mit anderen IT-Systemen,
    - die Rechte betroffener Personen und verfügbare Rechtsbehelfe,
    - die unabhängige Überprüfung der Bedingungen für den Zugriff durch Gefahrenabwehr- und Strafverfolgungsbehörden,
    - die Verteilung von Rollen und Verantwortlichkeiten auf EAGK und eu-LISA,
    - die Überprüfung durch die ETIAS-Zentralstelle,
    - die Architektur und Informationssicherheit des ETIAS,
    - die vom System generierten Statistiken und
    - die Rolle des EDSB.

121. Der EDSB steht gerne für weitere Beratung zu dem Vorschlag 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, den 6. März 2017

Giovanni BUTTARELLI
Europäischer Datenschutzbeauftragter

VERWEISE

[1] ABl. L 281 vom 23.11.1995, S. 31.
[2] ABl. L 8 vom 12.1.2001, S. 1.
[3] ABl. L 350 vom 30.12.2008, S. 60.
[4] Mitteilung vom 13. Februar 2008 der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen „Vorbereitung der nächsten Schritte für die Grenzverwaltung in der Europäischen Union“, KOM(2008) 69 endg.
[5] Vorläufige Kommentare des EDSB vom 3. März 2009, abrufbar unter https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Comments/2008/08-03-03_Comments_border_package_EN.pdf.
[6] Policy study on an EU Electronic System for travel Authorization (Studie über ein System zur elektronische Erteilung von Reisebewilligungen) (EU ESTA) aus dem Februar 2011, abrufbar unter: http://ec.europa.eu/dgs/home-affairs/e-library/docs/pdf/esta_annexes_en.pdf.
[7] Mitteilung vom 25. Oktober 2011 der Kommission an das Europäische Parlament und den Rat „Intelligente Grenzen: Optionen und weiteres Vorgehen“, KOM(2011) 680 endg.
[8] Mitteilung vom 6. April 2016 der Kommission an das Europäische Parlament und den Rat „Solidere und intelligentere Informationssysteme für das Grenzmanagement und mehr Sicherheit“, COM(2016) 205 final.
[9] Machbarkeitsstudie vom 16. November 2016 für ein Europäisches Reiseinformations- und -genehmigungssystem (ETIAS) - Abschlussbericht abrufbar unter: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/legislative-documents/docs/20161116/etias_feasability_study_en.pdf.
[10] 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, ABl. L 119 vom 4.5.2016, S. 1.
[11] 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, ABl. L 119 vom 4.5.2016, S. 89.
[12] 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.
[13] Vorschlag für eine Vorordnung des Europäischen Parlaments und des Rates 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.
[14] Verordnung (EU) 2016/1624 des Europäischen Parlaments und des Rates vom 14. September 2016 über die Europäische Grenz- und Küstenwache und zur Änderung der Verordnung (EU) 2016/399 des Europäischen Parlaments und des Rates sowie zur Aufhebung der Verordnung (EG) Nr. 863/2007 des Europäischen Parlaments und des Rates, der Verordnung (EG) Nr. 2007/2004 des Rates und der Entscheidung des Rates 2005/267/EG, ABl. L 251 vom 16.9.2016, S. 1.
[15] Einschließlich beispielsweise von Treffer/kein Treffer-Informationen und Antworten auf Hintergrundfragen zu Gesundheit, strafrechtlichen Verurteilungen, Aufenthalt in einem bestimmten Kriegs- oder Konfliktgebiet.
[16] In Artikel 3 Absatz 1 des Vorschlags ist das „Risiko für die öffentliche Gesundheit“ definiert als *„eine Gefahr für die öffentliche Gesundheit im Sinne des Artikel 2 Nummer 21 der Verordnung (EU) 2016/399“*, also als *„eine Krankheit mit epidemischem Potenzial im Sinne der Internationalen Gesundheitsvorschriften der Internationalen Gesundheitsorganisation (WHO) und sonstige übertragbare, durch Infektionserreger oder*

Parasiten verursachten Krankheiten, sofern gegen diese Krankheiten Maßnahmen zum Schutz der Staatsangehörigen der Mitgliedstaaten getroffen werden“.

[17] Siehe weiter oben Kapitel III, Abschnitt 2. Festlegung der Ziele.

[18] Siehe z. B. *Profiling the European Citizen. Cross-Disciplinary Perspectives*, eds. M. Hildebrandt, S. Gutwirth, Springer 2008, *Legal Implications of Data Mining: Assessing the European Union's Data Protection Principles in Light of the United States Government's National Intelligence Data Mining Practices*, L. Colonna, Stockholm 2016.

[19]Es besteht lediglich eine kleine Ausnahme für Familienangehörige von EU-Bürgern oder Drittstaatsangehörigen, die nach dem Unionsrecht das Recht auf Freizügigkeit genießen (siehe Artikel 21 des Vorschlags).

[20] In Artikel 4 Absatz 15 der Datenschutz-Grundverordnung sind Gesundheitsdaten definiert als *„personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen“.* Sie fallen unter strengere Datenschutzregelungen, die für besondere Kategorien von Daten gelten. Für den Fall, dass die Verarbeitung solcher Daten aus Gründen eines erheblichen öffentlichen Interesses erforderlich ist, sieht Artikel 9 DSGVO vor, dass das Unionsrecht oder das Recht eines Mitgliedstaats angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen betroffener Personen vorsieht.

[21] Siehe Machbarkeitsstudie von 2016, *op. cit.*, Tabelle 41, S. 131.

[22] EDSB, Stellungnahme vom 7. Oktober 2009 über den Zugang zu Eurodac zu Strafverfolgungszwecken, Punkt 18; EDSB, Stellungnahme vom 18. Juli 2013 zu den Vorschlägen für eine Verordnung über ein Einreise-/Ausreisesystem (EES) und für eine Verordnung über ein Registrierungsprogramm für Reisende (RTP), Punkt 68; Formelle Kommentare des EDSB zur öffentlichen Konsultation zum Thema Intelligente Grenzen, S. 5; EDSB, Stellungnahme 06/2016 zum zweiten Paket „Intelligente Grenzen“ der EU, Punkt 76.

[23] Begründung, S. 11.

[24] Siehe Artikel 5 und die Artikel 9 bis 14 der Verordnung (EG) Nr. 767/9 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.

[25] Begründung, S. 11.

[26] Der EGMR befand, dass der Begriff Notwendigkeit nicht so flexibel ist wie „zulässig“, „normal“ oder „hilfreich“, dass er aber „ein dringendes gesellschaftliches Bedürfnis impliziert“; siehe EGMR, Handyside gegen Vereinigtes Königreich, 7. Dezember 1976, Beschwerde Nr. 5493/72, Rn. 48.

[27] Bericht der Kommission an das Europäische Parlament und den Rat über die Durchführung der Verordnung (EG) Nr. 767/2008 über das Visa-Informationssystem (VIS), die Verwendung von Fingerabdrücken an den Außengrenzen und die Verwendung biometrischer Daten im Visumantragsverfahren/REFIT-Evaluierung, S. 11.

[28] EDSB, Stellungnahme 06/2016 vom 21. September 2016 zum zweiten Paket „Intelligente Grenzen“, Punkt 14.

[29] Siehe Machbarkeitsstudie von 2016, *op. cit.*, S. 156-158.

[30] Siehe EDSB, Stellungnahme 06/2016 zum zweiten Paket „Intelligente Grenzen“, Punkt 28.

[31] Siehe Machbarkeitsstudie von 2016, *op. cit.*, S. 15.

[32] Aus der Sicht des EDSB würde die Datenspeicherfrist der Gültigkeitsdauer der Reisegenehmigung – im Einklang mit Artikel 47 Absatz 1 Buchstabe a – nur in wenigen (unwahrscheinlichen) Fällen entsprechen, in denen im Zusammenhang mit der Genehmigung kein Einreisedatensatz im EES gespeichert wird. Dies könnte eintreten, wenn ein von der Visumpflicht befreiter Reisender zwar eine ETIAS-Reisegenehmigung erhalten hat, diese aber während der Gültigkeitsdauer nicht genutzt hat oder an dem selben Tag, an dem die ETIAS-Genehmigung erteilt wurde, in den Schengen-Raum eingereist ist oder ihm trotz der Genehmigung die Einreise in den Schengen-Raum verweigert wurde.

[33] Begründung, S. 34.

[34] EDSB, Stellungnahme 06/2016 zum zweiten Paket „Intelligente Grenzen“, Punkt 29.

[35] Verordnung (EU) Nr. 604/2013 des Europäischen Parlaments und des Rates vom 26. Juni 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, ABl. L 180 vom 29.6.2013, S. 31.

[36] Siehe Artikel 28 des Vorschlags für eine Verordnung des Europäischen Parlaments und des Rates über den 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, COM(2017) 8 final.

[37] Begründung, S. 12.

[38] EDSB, Stellungnahme 06/2016 zum zweiten Paket „Intelligente Grenzen“, Punkt 86; EDSB, Stellungnahme 07/2016 vom 21. September 2016 zum ersten Reformpaket für das Gemeinsame Europäische Asylsystem, Punkt 58.
[39] Verordnung (EU) 2016/794 des Europäischen Parlaments und des Rates vom 11. Mai 2016 über die Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol) und zur Ersetzung und Aufhebung der Beschlüsse 2009/371/JI, 2009/934/JI, 2009/935/JI, 2009/936/JI und 2009/968/JI, ABl. L 135 vom 24.5.2016, S. 53.
[40] Verordnung (EU) 2016/794, Artikel 44 Absatz 4.
[41] *Ebenda.*
[42] Dies kann vorkommen, weil Treffer nicht auf genauen Übereinstimmungen beruhen, sondern auf Ähnlichkeiten zwischen den Informationen im Antragsdatensatz und den Informationen in der abgefragten Datenbank, oder weil bei einer Abfrage unter Verwendung mehrerer Attribute aus dem Antragsdatensatz lediglich einige von ihnen den Informationen in der abgefragten Datenbank entsprechen.

[43] Artikel 20 des Vorschlags – Überprüfung durch die ETIAS-Zentralstelle
[44] Artikel 6 des Vorschlags – Aufbau und technische Architektur des ETIAS-Informationssystems
[45] Alle in Artikel 10 des Vorschlags (Interoperabilität mit anderen Informationssystemen) aufgeführten.
[46] Artikel 14 des Vorschlags – Die öffentliche Website und die mobile App für Mobilgeräte.
[47] Artikel 39 des Vorschlags – Datenzugriff durch Beförderungsunternehmer zu Überprüfungszwecken.
[48] Artikel 73 des Vorschlags – Verwendung von Daten zur Erstellung von Berichten und Statistiken.
[49] Im Einklang mit Artikel 22 der Verordnung (EG) Nr. 45/2001.
[50] Nach Artikel 23 der Verordnung (EG) Nr. 45/2001 müsste eu-LISA auch den in Artikel 22 festgelegten Pflichten des für die Verarbeitung Verantwortlichen nachkommen: „*Die Durchführung einer Verarbeitung im Auftrag erfolgt auf der Grundlage eines Vertrags oder Rechtsakts, durch den der Auftragsverarbeiter an den für die Verarbeitung Verantwortlichen gebunden ist und in dem insbesondere Folgendes vorgesehen ist: a) Der Auftragsverarbeiter handelt nur auf Weisung des für die Verarbeitung Verantwortlichen; b) die in den Artikeln 21 und 22 genannten Verpflichtungen gelten auch für den Auftragsverarbeiter [...]“.*
[51] Dies wird in Artikel 49 Absatz 1 des Vorschlags bekräftigt, wo wiederholt wird, dass sowohl eu-LISA als auch die Europäische Agentur für die Grenz- und Küstenwache der Verordnung (EG) Nr. 45/2001 unterliegen; damit ist der EDSB ihre Aufsichtsbehörde bei der Verarbeitung personenbezogener Daten.
[52] Artikel 47 Absatz 2 der Verordnung (EG) Nr. 45/2001 und die Nachfolgebestimmung (Artikel 59 Absatz 1) weisen Ähnlichkeit auf mit dem Vorschlag vom 10. Januar 2017 für eine Verordnung des Europäischen Parlaments und des Rates über den 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, COM(2017) 8 final.
[53] Hierzu sollte der EDSB als Empfänger der Berichte aufgeführt werden, die in den folgenden Artikeln erwähnt werden: Artikel 77 Absatz 3, Artikel 78 Absatz 4, Artikel 81 Absatz 2, Artikel 81 Absatz 4 und Artikel 81 Absatz 5. Artikel 52 Absatz 4 sollte ferner besagen, dass der EDSB über die Maßnahmen unterrichtet wird, die eu-LISA gemäß Artikel 52 ergreift, und zwar nicht nur bei der Inbetriebnahme des ETIAS, sondern während des gesamten Lebenszyklus des ETIAS und seiner Daten.