STELLUNGNAHME DES EDSB ZUR ETIAS-DSFA (Fall 2021-0640)

1. EINLEITUNG

- Die vorliegende Stellungnahme befasst sich mit der Datenschutz-Folgenabschätzung (im Folgenden „DSFA“) von eu-LISA für das Europäische Reiseinformations- und -genehmigungssystem (im Folgenden „ETIAS“).

- Der EDSB gibt diese Stellungnahme gemäß Artikel 57 Absatz 1 Buchstabe g und Artikel 58 Absatz 3 Buchstabe c der Verordnung (EU) 2018/1725[1] (im Folgenden „Verordnung“) ab.

2. HINTERGRUND

Das ETIAS wird durch die Verordnung (EU) 2018/1240[2] (im Folgenden „ETIAS-Verordnung“) eingerichtet. Es wird personenbezogene Daten über von der Visumpflicht befreite Reisende in die Schengen-Staaten erfassen und speichern, um festzustellen, ob von diesen Reisenden ein Risiko für die Sicherheit, ein Risiko der irregulären Einwanderung oder ein Epidemierisiko ausgeht.

---

[1] Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG, ABl. L 295 vom 21.11.2018, S. 39.

[2] Verordnung (EU) 2018/1240 des Europäischen Parlaments und des Rates vom 12. September 2018 über die Einrichtung eines Europäischen Reiseinformations- und -genehmigungssystems (ETIAS) und zur Änderung der Verordnungen (EU) Nr. 1077/2011, (EU) Nr. 515/2014, (EU) 2016/399, (EU) 2016/1624 und (EU) 2017/2226, ABl. L 236 vom 19.9.2018, S. 1.

Das ETIAS wird aus einem IT-Großsystem bestehen, das sich aus dem (von eu-LISA entwickelten) ETIAS-Informationssystem[3], der ETIAS-Zentralstelle[4] (die in der Europäischen Agentur für die Grenz- und Küstenwache (Frontex) eingerichtet wird) und den nationalen ETIAS-Stellen[5] (die bei einer in jedem Mitgliedstaat benannten zuständigen Behörde angesiedelt werden)[6] zusammensetzt. Das ETIAS-Informationssystem besteht aus mehreren Elementen, darunter das ETIAS-Zentralsystem (einschließlich der Überwachungsliste), einheitliche nationale Schnittstellen, eine Kommunikationsinfrastruktur, ein Zugang für Beförderungsunternehmen usw.[7]

Nach der ETIAS-Verordnung entwickelt eu-LISA das ETIAS-Informationssystem und sorgt für seine technische Verwaltung.[8] In diesem Zusammenhang ist eu-LISA verpflichtet, während des gesamten Lebenszyklus der Entwicklung des ETIAS die Grundsätze des eingebauten Datenschutzes und der datenschutzfreundlichen Grundeinstellungen zu befolgen.[9] Der EDSB hält fest, dass der Begriff „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen" das weit gefasste Konzept technischer Maßnahmen zur Gewährleistung der Privatsphäre bezeichnet. In dieser Stellungnahme verwendet der EDSB den in Artikel 27 der Verordnung genannten Begriff „Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen", wonach der Verantwortliche technische und organisatorische Maßnahmen zur Umsetzung der Datenschutzgrundsätze ergreifen muss.[10]

Zusätzlich zu seiner Rolle als Entwickler des Systems wird in den Artikeln 57 und 58 der ETIAS-Verordnung eu-LISA als Verantwortlicher für das

---

[3] Artikel 6 der ETIAS-Verordnung.
[4] Artikel 7 der ETIAS-Verordnung.
[5] Artikel 8 der ETIAS-Verordnung.
[6] Artikel 3 der ETIAS-Verordnung.
[7] Artikel 6 Absatz 2 der ETIAS-Verordnung.
[8] Artikel 6 Absatz 1 und Artikel 73 der ETIAS-Verordnung.
[9] Artikel 73 Absatz 3 der ETIAS-Verordnung.
[10] Zwar dürften auch nach Artikel 27 der Verordnung ergriffene Maßnahmen dazu beitragen, dass das eher allgemeine Ziel des „Schutzes der Privatsphäre durch Technikgestaltung" erreicht wird, doch sind wir der Auffassung, dass bezüglich des Ziels „Schutz der Privatsphäre durch Technikgestaltung" ein breiteres Spektrum von Ansätzen berücksichtigt werden könnte, denn es umfasst ja, im Einklang mit den in der Charta der Grundrechte der EU verankerten Grundsätzen und Werten, auch eine visionäre und ethische Dimension. (EDSB, Vorläufige Stellungnahme zu Schutz der Privatsphäre durch Technikgestaltung (Stellungnahme 5/2018)), abrufbar unter: https://edps.europa.eu/sites/default/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf)

Informationssicherheitsmanagement des ETIAS-Zentralsystems und als Auftragsverarbeiter für die Verarbeitung personenbezogener Daten im ETIAS-Informationssystem benannt.

Frontex (die Europäische Agentur für die Grenz- und Küstenwache) gilt in Bezug auf die Verarbeitung personenbezogener Daten im ETIAS-Zentralsystem als Verantwortlicher, während die nationale ETIAS-Stelle jedes Mitgliedstaats für die Verarbeitung personenbezogener Daten im ETIAS-Zentralsystem durch diesen Mitgliedstaat als Verantwortlicher gilt.[11]

Angesichts des Umfangs und der Komplexität des ETIAS organisierte der EDSB am 6. Dezember 2019 und am 24. März 2020 zwei Treffen mit Mitarbeitern von Frontex und eu-LISA (einschließlich ihrer Datenschutzbeauftragten) sowie mit Bediensteten der EU-Kommission.[12] Ziel dieser Sitzungen war es, ein klares Verständnis des laufenden Verfahrens für die Entwicklung des ETIAS zu erlangen, insbesondere im Hinblick auf die Ausarbeitung der Datenschutz-Folgenabschätzung (DSFA), die ein Schlüsselinstrument für die ordnungsgemäße Umsetzung der Grundsätze des Datenschutzes durch Technikgestaltung und datenschutzfreundliche Voreinstellungen ist.

Die Erstellung der DSFA ist eine Verpflichtung des für eine bestimmte Datenverarbeitung Verantwortlichen. Im Falle von ETIAS obliegt diese Verpflichtung gemeinsam Frontex, den nationalen ETIAS-Stellen und eu-LISA. Als gemeinsam für die Verarbeitung Verantwortliche des ETIAS sollte jeder von ihnen nicht nur auf die mit seinen eigenen Datenverarbeitungsvorgängen innerhalb des Systems verbundenen Datenschutzrisiken eingehen, sondern auch auf die Risiken im Zusammenhang mit seinen Interaktionen mit anderen Datenschutzvorgängen und anderen Systemen. Diese DSFA können daher nicht getrennt voneinander durchgeführt werden.

Aus diesen Gesprächen ging hervor, dass eu-LISA in ihrer Eigenschaft als Entwicklerin des Systems[13] die Verantwortung für die Koordinierung der gesamten technischen Entwicklung des Systems, einschließlich der DSFA, übernommen hatte.[14]

---

[11] Artikel 57 der ETIAS-Verordnung.

[12] Treffen auf Arbeitsebene fanden am 6. Dezember 2019 (mit Frontex und eu-LISA) und am 24. März 2020 (mit Frontex, eu-LISA und der EU-Kommission) statt.

[13] Artikel 6 und 73 der ETIAS-Verordnung.

[14] Sitzung auf Arbeitsebene am 24. März 2020 (mit Frontex, eu-LISA und der EU-Kommission).

Daraufhin übermittelte der EDSB am 13. Mai 2020 eine vorläufige Orientierungshilfe an eu-LISA in Bezug auf die ETIAS-DSFA[15], die die bereits in seinem Toolkit zur Rechenschaftspflicht enthaltenen Leitlinien ergänzt. [16]

Am 17. Juni 2021 ersuchte eu-LISA um eine Stellungnahme des EDSB zu der von ihr für das ETIAS durchgeführten DSFA und wies darauf hin, dass es sich bei dem zur Konsultation übermittelten Dokument um die endgültige Fassung der DSFA handelt.

3. ANALYSE DER DSFA

3.1. Erfordernis einer DSFA nach Artikel 39 der Verordnung

Nach Artikel 39 der Verordnung ist der Verantwortliche, wenn eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, gehalten, vor der Verarbeitung eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchzuführen.

Nach Artikel 39 Absatz 4 der Verordnung erstellt der EDSB eine Liste der Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist.[17] eu-LISA hat zwei Verarbeitungsvorgänge aus dieser Liste ermittelt (nämlich „Ausschlussdatenbanken“ und „umfassende Verarbeitung besonderer Kategorien personenbezogener Daten“), die das Erfordernis einer DSFA begründen.[18]

Nach Auffassung des EDSB sollte eu-LISA etwas näher erläutern, warum sie gerade diese beiden Verarbeitungsvorgänge im Rahmen des ETIAS ermittelt hat. Einer solchen

---

[15] Schreiben an den Datenschutzbeauftragten von eu-LISA vom 13. Mai 2020 (DH/GC/vm/D(2020) 1207 C 2019-0495).

[16] Das Toolkit des EDSB zur Rechenschaftspflicht besteht aus drei Dokumenten:

- einer Zusammenfassung: Leitfaden für Organe, Einrichtungen und Agenturen der Union über die Dokumentierung von Verarbeitungsvorgängen
- Teil I: Verzeichnisse, Register und Erfordernis einer Datenschutz-Folgenabschätzung und
- Teil II: Datenschutz-Folgenabschätzung und vorherige Konsultation.

Diese Dokumente sind abrufbar unter https://edps.europa.eu/node/4582_en.

[17] Entscheidung des Europäischen Datenschutzbeauftragten vom 16. Juli 2019 über gemäß Artikel 39 Absätze 4 und 5 der Verordnung (EU) 2018/1725 erstellte DSFA-Listen

[18] Siehe Tabelle 4 „Rechtsgrundlage“ auf S. 20f. der DSFA.

Erläuterung kommt besondere Bedeutung zu, da sie eine erste Analyse der Risiken bietet, die sich aus der Nutzung des Systems ergeben, und denen die DSFA durch die Festlegung von Risikoeindämmungsmaßnahmen sorgfältig Rechnung tragen muss.

In diesem Zusammenhang weist der EDSB auf seine nicht erschöpfende Liste von Kriterien hin, anhand deren beurteilt werden kann, ob Verarbeitungsvorgänge wahrscheinlich ein hohes Risiko zur Folge haben[19], sowie auf sein „Toolkit zur Rechenschaftspflicht"[20].

Mit Blick auf die Erläuterung betreffend die Durchführung einer DSFA stellt der EDSB fest, dass das ETIAS riesige Mengen personenbezogener Daten (auch zu Straftaten) von Millionen Menschen erheben und verarbeiten und diese Daten mit Daten abgleichen wird, die in mehreren anderen IT-Großsystemen, einschließlich zentraler Datenbanken für die Zusammenarbeit der Strafverfolgungsbehörden, gespeichert sind. Diese Daten werden zur Unterstützung von Entscheidungen herangezogen, die sich auf Personen nachteilig auswirken können. Darüber hinaus wird für die Erstellung von Profilen betroffener Personen und die automatische Bestimmung potenziell risikobehafteter Personen, für die eine manuelle Bearbeitung ihrer Anträge erforderlich ist, eine Reihe von Überprüfungsregeln angewandt.

Die Auswirkungen könnten erheblich sein, da die Verweigerung der Einreise in das Schengen-Gebiet auf der Grundlage der Datenverarbeitung im ETIAS eine Reihe nachteiliger Folgen für Personen haben könnte. Zu diesen Folgen gehören die Einschränkung des Rechts auf Freizügigkeit, finanzielle Auswirkungen, wenn sie zu Geschäftszwecken in die EU reisen, oder Gesundheitsprobleme, wenn sie in die EU wegen einer medizinischen Behandlung reisen, die sie in ihrem eigenen Land nicht erhalten können. Darüber hinaus kann der Zugriff von Strafverfolgungsbehörden auf die im ETIAS gespeicherten Daten auch Personen schaden, die dann in den Mittelpunkt der Aufmerksamkeit der Strafverfolgungsbehörden rücken und Gegenstand von Ermittlungsmaßnahmen werden könnten.

Vor diesem Hintergrund ist der EDSB der Auffassung, dass eu-LISA die ermittelten Arten von Verarbeitungsvorgängen, die zu der Entscheidung über die Durchführung einer DSFA führen,

---

[19]Entscheidung des Europäischen Datenschutzbeauftragten vom 16. Juli 2019 über gemäß Artikel 39 Absätze 4 und 5 der Verordnung (EU) 2018/1725 erstellte DSFA-Listen

[20]Insbesondere enthält Kapitel 4 des Toolkits zur Rechenschaftspflicht (Teil I) Kriterien für die Entscheidung, ob eine DSFA zwingend vorgeschrieben ist, sowie eine Liste riskanter Verarbeitungsvorgänge.

näher erläutern sollte, indem sie beispielsweise der nicht erschöpfenden Liste von Kriterien für die Einschätzung, ob Verarbeitungsvorgänge wahrscheinlich ein hohes Risiko zur Folge haben, Rechnung trägt.

Eine sorgfältige Ermittlung von Kriterien für ein hohes Risiko kann dem DSFA-Team helfen, denn sie ermöglicht einen Überblick über die Indikatoren für ein hohes Risiko, die bei der Einschätzung berücksichtigt werden sollten. Dies bietet auch eine gute Möglichkeit, die Mitarbeiter von eu-LISA zu schulen und sicherzustellen, dass in Zukunft keine Kriterien verfehlt werden, was zu ungerechtfertigten Entscheidungen über die Nichtdurchführung einer DSFA führen könnte, während die entsprechende Datenverarbeitung ein hohes Risiko für die Grundrechte betroffener Personen bergen könnte.

Der EDSB empfiehlt eu-LISA, die ermittelten Arten von Verarbeitungsvorgängen, die zu der Entscheidung über die Durchführung einer DSFA führen, näher zu erläutern und dabei die nicht erschöpfende Liste von Kriterien zu berücksichtigen, anhand deren beurteilt werden kann, ob Verarbeitungsvorgänge wahrscheinlich zu hohen Risiken führen.

3.2. Aufbau der DSFA

Der EDSB begrüßt, dass die DSFA in ihrem Aufbau generell dem Muster der im „Toolkit zur Rechenschaftspflicht“ des EDSB bereitgestellten DSFA entspricht.[21] Nach einer detaillierten Analyse der einzelnen Elemente der DSFA mit dem Ziel, festzustellen, ob sie die in der Verordnung geforderten Informationen liefern, wie sie im Toolkit zur Rechenschaftspflicht weiterentwickelt wurden, formulieren wir in den nachstehenden Abschnitten die folgenden Empfehlungen und Verbesserungsvorschläge.

3.3. Anwendungsbereich der DSFA

In der Zusammenfassung hat eu-LISA eine Beschreibung des Anwendungsbereichs der DSFA gegeben. Darin heißt es insbesondere: „Diese DSFA bewertet die bei der Gestaltung und

[21] Siehe Anhang III des Toolkits, Teil II.

Entwicklung des ETIAS ermittelten Datenschutzrisiken. Es handelt sich um eine erste Studie, die durch synergetische Beiträge von Frontex und den Mitgliedstaaten ergänzt werden muss, um eine umfassende Abschätzung aller Risiken im Zusammenhang mit der Einrichtung des ETIAS zu erhalten" (S. 8). Gleichzeitig hebt die Risikoanalyse im Wesentlichen auf die Zuständigkeiten von eu-LISA für die Gestaltung, die Entwicklung und das Informationssicherheitsmanagement des ETIAS ab.

Der EDSB geht davon aus, dass angesichts der Komplexität des Systems und der unterschiedlichen Rollen der beteiligten Akteure die bei ihm eingegangene DSFA nicht die endgültige Fassung der ETIAS-DSFA ist. Da eu-LISA die Umsetzung des Systems koordiniert und den Grundsatz des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen anwendet, ist eu-LISA auch dafür verantwortlich, diese DSFA anhand der von den Mitgliedstaaten und von Frontex erhaltenen Beiträge zu den in deren jeweiligen DSFA ermittelten Risiken zu aktualisieren.

Der EDSB empfiehlt eu-LISA, vor der Inbetriebnahme des Systems eine umfassende DSFA zu erstellen, die die von allen Interessenträgern (d. h. Frontex, Mitgliedstaaten, Europol, eu-LISA) ermittelten Risiken und die Risiken, die sich aus der Entwicklung und dem Betrieb des ETIAS ergeben, umfasst.

3.4. Proaktive Ermittlung von Risiken durch die wichtigsten beteiligten Akteure

Angesichts der Komplexität des ETIAS, insbesondere im Hinblick auf seine Verknüpfungen mit anderen Systemen und der Schlüsselrolle mehrerer Interessenträger, ist es von entscheidender Bedeutung, eine gute Koordinierung zwischen allen Interessenträgern sicherzustellen, damit geeignete Strategien zur Bewältigung aller ermittelten Risiken ausgearbeitet werden können. Am ETIAS sind im Wesentlichen drei Akteure beteiligt: eu-LISA, Frontex (die ETIAS-Zentralstelle) und die Mitgliedstaaten (die nationalen ETIAS-Stellen). Aber auch Europol ist ein wichtiger am ETIAS beteiligter Akteur, da es Daten in die

ETIAS-Überwachungsliste[22] eingeben und dem ETIAS-Überprüfungsausschuss angehören wird, der Frontex in Bezug auf die ETIAS-Überprüfungsregeln berät[23].

Bei der Konzeption und Gestaltung des ETIAS muss eu-LISA alle Risiken berücksichtigen, die sich für die betroffenen Personen aus der Nutzung des Systems insgesamt ergeben. Erst wenn das ETIAS betriebsbereit ist, werden einige Teile der Verarbeitung in die Zuständigkeit und Verantwortung von Frontex (der ETIAS-Zentralstelle) und der Mitgliedstaaten (nationale ETIAS-Stellen) fallen.

Frontex und die Mitgliedstaaten müssen vor der Inbetriebnahme des ETIAS eigene DSFA in Bezug auf ihre Verarbeitungstätigkeiten durchführen. Diese können jedoch einige neue funktionale Anforderungen für das ETIAS im Rahmen von Risikoeindämmungsmaßnahmen mit sich bringen. Abgesehen davon, dass diese zu einem späteren Zeitpunkt der Gestaltung zu erwarten sind, sollte eu-LISA bei der Ermittlung solcher Risiken und der Art und Weise, wie das System zur Vermeidung oder Eindämmung dieser Risiken beitragen könnte, eine proaktive unterstützende Haltung einnehmen. Hilfreich in dieser Richtung sind die Gesamtanalyse der Datenströme und die Einbeziehung der anderen Interessenträger in die Überarbeitung dieser DSFA.

Der DSFA ist zu entnehmen, dass eu-LISA mehrere externe Interessenträger (darunter Frontex, Vertreter der Mitgliedstaaten und Europol) konsultiert hat und dass das Ergebnis dieser Konsultationen in die Ausarbeitung der DSFA eingeflossen ist (Abschnitt 4.5.2). Allerdings hat der EDSB in der DSFA keine Beispiele für Risiken gefunden, die sich aus diesen Datenverarbeitungstätigkeiten oder aus den Interaktionen des Systems mit Verarbeitungsvorgängen im Zuständigkeitsbereich der ETIAS-Zentralstelle, der nationalen ETIAS-Stellen oder von Europol ergeben.

Beispiele für solche Risiken, die frühzeitig erkannt werden könnten, sind:

- Verzögerungen bei der manuellen Bearbeitung des ETIAS-Antrags durch die ETIAS-Zentralstelle, die nationale ETIAS-Stelle oder Europol (im Rahmen der Konsultation nach Artikel 29) oder bei der Bearbeitung von Anträgen betroffener Personen.

[22] Artikel 34 der ETIAS-Verordnung.
[23] Artikel 9 und 33 der ETIAS-Verordnung.

Obwohl in der ETIAS-Verordnung rechtliche Schwellenwerte für die Bearbeitung der Anträge berücksichtigt wurden, kann es dringliche Fälle geben, in denen Drittstaatsangehörige bereits vor Ablauf der Frist reisen müssen, aber aufgrund der manuellen Bearbeitung nicht reisen können. Im Rahmen der Eindämmung solcher Risiken sollten eu-LISA und die beteiligten Interessenträger prüfen, ob und wie das System zu Minimierung dieser Risiken beitragen könnte, beispielsweise durch die Bereitstellung von Berichten über anhängige Anträge oder durch Warnmeldungen für Anträge, bei denen entweder die Frist demnächst abläuft oder das Reisedatum naht.

- Fehler oder Verzögerungen bei der manuellen Bearbeitung des ETIAS-Antrags aufgrund nicht ausreichend geschulter Mitarbeiter, die dazu führen, dass Drittstaatsangehörige nicht reisen können.

  Im Rahmen der Eindämmung solcher Risiken sollten eu-LISA und die beteiligten Interessenträger prüfen, ob und wie das System dazu beitragen könnte, solche Fehler von Bediensteten, die das System nutzen, zu erkennen, beispielsweise durch die Bereitstellung von Statistiken darüber, wie viele Anträge der Nutzer im Vergleich zu den Folgeeinreiseanträgen des Drittstaatsangehörigen abgelehnt hat.

- Risiken im Zusammenhang mit der Datenqualität, wie Fehler bei Daten, die von den Mitgliedstaaten und/oder Europol in die ETIAS-Überwachungsliste oder in andere vom ETIAS-System abgefragte Datenbanken eingegeben wurden (5.5.-automatisierte Verarbeitung).

  Eu-LISA und die beteiligten Interessenträger sollten prüfen, ob und wie das System dazu beitragen könnte, solche Fehler zu erkennen.

Der EDSB empfiehlt, in die DSFA Risiken im Zusammenhang mit den Interaktionen des Systems mit Verarbeitungsvorgängen unter der Verantwortung anderer Interessenträger (d. h. der ETIAS-Zentralstelle, der nationalen ETIAS-Stellen und/oder Europol) in enger Abstimmung mit ihnen aufzunehmen.

3.5. Beschreibung der Verarbeitung

Die Festlegung des Kontexts und die Beschreibung der Verarbeitungsvorgänge bilden die Grundlage einer soliden DSFA und sind von wesentlicher Bedeutung, um die Risiken für die Grundrechte des Einzelnen angemessen zu erkennen. Wie im Toolkit zur Rechenschaftspflicht[24] hervorgehoben, sollte die Beschreibung dem Leser (z. B. den von der Verarbeitung betroffenen Personen, dem EDSB oder anderen Interessenträgern) ein klares Verständnis der Verarbeitungsvorgänge ermöglichen, einschließlich der Gründe und der Art und Weise ihrer Durchführung.

Konkret sollte die Beschreibung Folgendes umfassen:

- ein Datenflussdiagramm des Prozesses (Ablaufdiagramm): Was wird wo/bei wem erhoben, was geschieht damit, wo wird es gespeichert, an wen wird es weitergegeben?
- eine Beschreibung des Zwecks/der Zwecke der Verarbeitung: Wie bei den anderen Elementen sollte diese Erläuterung schrittweise erfolgen, wobei erforderlichenfalls zwischen Zwecken zu unterscheiden ist;[25]
- Beschreibung des Zusammenspiels mit anderen Verarbeitungsvorgängen: Werden für diesen Verarbeitungsvorgang personenbezogene Daten aus anderen Systemen verarbeitet? Werden personenbezogene Daten aus diesem Verarbeitungsvorgang in anderen Verarbeitungsvorgängen wiederverwendet?
- eine Beschreibung der unterstützenden Infrastruktur: Datenbanken, Integration neuer Technologien usw.

Kapitel 4 der DSFA soll eine allgemeine Beschreibung der Verarbeitung bieten, während in Kapitel 5 die verschiedenen Verarbeitungstätigkeiten ausführlicher dargestellt werden.

Angesichts der Komplexität des Systems hält es der EDSB für angemessen, einen Top-down-Ansatz zu verfolgen, also zunächst das Gesamtbild mit den wichtigsten Verarbeitungsvorgängen zu beschreiben und dann zu einer detaillierteren und spezifischeren Beschreibung dieser Vorgänge überzugehen. Wie im Folgenden weiter ausgeführt

[24] Siehe EDSB, Toolkit zur Rechenschaftspflicht, Teil I, S. 7.

[25] Im Rahmen dieser Beschreibung sollte kurz erläutert werden, warum die Organisation diesen Verarbeitungsvorgang durchführen muss und wie sie sich auf das für das Ziel der Verarbeitung erforderliche Maß beschränkt (Erforderlichkeit und Verhältnismäßigkeit).

(Ziffern 3.5.1 und 3.5.2), stellt der EDSB jedoch fest, dass das Gesamtbild unvollständig ist, dass einige Zwischenschritte fehlen und einige spezifische Schritte nicht detailliert genug dargestellt sind, um eine klare Visualisierung und ein klares Verständnis des Systems zu erhalten.

3.5.1. Allgemeine Beschreibung (Kapitel 4 der DSFA)

Der EDSB hält fest, dass in Kapitel 4 viele Elemente einer allgemeinen Beschreibung der Datenverarbeitungstätigkeit aufgeführt werden. Allerdings ermöglicht die Art und Weise, wie sie dargestellt und beschrieben werden, kein klares, problemloses und umfassendes Verständnis der Datenverarbeitungstätigkeit. Verschärft wird dies durch das Fehlen eines Datenflussdiagramms, aus dem hervorgeht, wie personenbezogene Daten das System durchlaufen (woher die Daten stammen, wohin sie gehen, wie sie sich ändern und wo sie letztendlich landen).

Der EDSB betont, wie wichtig eine klare Visualisierung des gesamten Systems ist. Sie könnte mit einer umfassenden Betrachtung des Systems beginnen, das dann in die wichtigsten Datenverarbeitungsvorgänge zerlegt wird, die wiederum in Teilprozesse unterteilt werden. Datenflussdiagramme könnten in mehreren miteinander verschachtelten Schichten erstellt werden. Ein einzelner Prozess auf einem übergeordneten Diagramm könnte vergrößert werden, um ein detaillierteres Datenflussdiagramm zu ergeben. Mit anderen Worten: Es könnte eine Hierarchie von Datenflussdiagrammen erstellt werden, die mit einer abstrakten Betrachtung des Systems beginnt und mit einer Reihe von Diagrammen endet, die die Teilprozesse der untersten Ebene darstellen.

Die oberste Ebene („Ebene 0“) könnte einfach das System, die externen Einrichtungen, mit denen es interagiert, und die Datenströme zwischen dem System und den externen Stellen aufzeigen. Die erste Ebene könnte die wichtigsten Datenverarbeitungsvorgänge umfassen, während auf einer zweiten Ebene die wichtigsten Verarbeitungsvorgänge vertieft würden. Der EDSB stellt fest, dass in der DSFA die Datenflussdiagramme der „Ebene 0“ und der „ersten Ebene“ fehlen, die eine klare Visualisierung und ein klares Verständnis des Systems ermöglichen.

Die zusammenfassende Übersicht über das ETIAS auf S. 29 bietet zwar einen guten Überblick über die Systemkomponenten und gibt damit Aufschluss über die Systemarchitektur, doch fehlt es an einer Visualisierung der Datenströme und der wichtigsten Datenverarbeitungsvorgänge.

Diese Visualisierung lässt sich auch aus der allgemeinen Beschreibung nur schwer herleiten.

Abschnitt 4.3 (Allgemeine Beschreibung der Datenverarbeitungstätigkeit) geht entweder zu detailliert auf bestimmte Aspekte ein (z. B. die Tatsache, dass die ETIAS-Zentralstelle rund um die Uhr betriebsbereit sein sollte) oder enthält unvollständige Angaben zu bestimmten Aspekten (z. B. Identifizierung externer Stellen).

Die Datenverarbeitung betreffende Informationen (z. B. erhobene Daten, Empfänger usw.) werden in Abschnitt 4.2 lediglich aufgeführt, jedoch nicht miteinander verknüpft. Dies ist jedoch von entscheidender Bedeutung, um einen umfassenden Überblick über die Datenverarbeitung zu erhalten. So tauchen beispielsweise nicht alle Empfänger der unter Punkt 4.3.4 aufgeführten Daten in der Beschreibung auf.

Darüber hinaus wurden in der Systembeschreibung mehrere zu erwartende Datenströme nicht gefunden. Beispiele hierfür sind der Widerruf der ETIAS-Reisegenehmigung (was dazu führen könnte, dass der Nutzer nicht benachrichtigt wird) oder die Überprüfung ihres Antrags oder ihrer ETIAS-Gültigkeitsdauer durch die Drittstaatsangehörigen.

Vor diesem Hintergrund empfiehlt der EDSB, in Kapitel 4 der DSFA zwei Datenflussdiagramme („Ebene 0“ und „erste Ebene“) hinzuzufügen, um eine klare Visualisierung der Art und Weise zu ermöglichen, wie Informationen im Allgemeinen in das System eingegeben und daraus gelöscht werden, welche Änderungen sie erfahren und wo die Informationen gespeichert werden. Das erste sollte das System, die externen Stellen, mit denen es interagiert, und die Datenströme zwischen dem System und den externen Stellen aufzeigen. Das zweite sollte eine Erweiterung des ersten sein und die wichtigsten Datenverarbeitungsvorgänge umfassen.

Der EDSB empfiehlt ferner, die Struktur von Kapitel 4 dahingehend zu überarbeiten, dass diese beiden Datenflussdiagramme klar, zielgerichtet und umfassend beschrieben werden können.

3.5.2. Systematische Beschreibung (Kapitel 5 der DSFA)

In Kapitel 5 werden die in der allgemeinen Beschreibung (siehe Kapitel 4) aufgeführten Hauptverarbeitungsvorgänge näher beschrieben. Dies könnte man als Datenflussdiagramm der „zweiten Ebene" betrachten.

Für jeden Hauptverarbeitungsvorgang sieht die DSFA Folgendes vor:
- ein Flussdiagramm,
- eine Tabelle mit den verschiedenen im Flussdiagramm genannten Schritten, einschließlich der einzelnen Schritte,
    - einen Verweis auf den Teilabschnitt, in dem jeder einzelne Schritt beschrieben wird,
    - den Zweck,
    - den den Daten zugrundeliegenden Wert,
- eine Beschreibung des Verfahrens für jeden Schritt,
- einen Gesamtüberblick.

Der EDSB begrüßt diesen Ansatz. Er stellt jedoch fest, dass es an Klarheit, Vollständigkeit und/oder Kohärenz mangelt.

Das Flussdiagramm, die Tabelle und die Beschreibungen der einzelnen Schritte sind nicht immer vorhanden oder aufeinander abgestimmt. So enthält z. B. Abschnitt 5.6 über die manuelle Verarbeitung keine Tabelle. In Abschnitt 5.5 werden die verschiedenen in der Tabelle genannten Schritte weder im Flussdiagramm noch in der Beschreibung aufgeführt (z. B. Offenlegung/Übermittlung der Daten). In Abschnitt 5.5 erscheinen Elemente aus der Gesamtübersicht nicht im Flussdiagramm (z. B. CIR) und umgekehrt (z. B. Überwachungsregeln). Die Nutzer, die die einzelnen Schritte ausführen, werden nicht immer angezeigt. Für ein und denselben Schritt wird eine andere Formulierung verwendet (z. B. wird in der Tabelle in Abschnitt 5.5 von „zusammengesetzten Datensätzen" gesprochen, während im Flussdiagramm und der Beschreibung von „konsolidiertem Ergebnis" die Rede ist.

Darüber hinaus sollten in der DSFA einige wichtige Datenverarbeitungsvorgänge genauer erläutert und beschrieben werden und nicht nur die Rechtsvorschriften abgeschrieben werden. So sollte beispielsweise in Abschnitt 5.5 über automatisierte Verarbeitungsvorgänge für jedes System (SIS, VIS usw.) beschrieben werden, welche Daten im Antrag des

Drittstaatsangehörigen für den Abgleich verwendet werden und welche Situationen (d. h. welche Daten oder Kombinationen von Daten) zu einem Treffer führen.

Vor diesem Hintergrund empfiehlt der EDSB, Folgendes sicherzustellen:
- für jeden Hauptdatenverarbeitungsvorgang sind ein Flussdiagramm, eine Tabelle und eine Beschreibung beigefügt,
- alle Schritte sind im Flussdiagramm und in der Tabelle aufgeführt und klar und einheitlich beschrieben,
- die Beschreibung jedes einzelnen Schritts umfasst den Nutzer, die Maßnahme, die Daten und den den Daten zugrundeliegenden Wert.

3.6. Bewertung der Notwendigkeit und Verhältnismäßigkeit

In Kapitel 6 der DSFA wird darauf hingewiesen, dass sie darauf abzielt, die Notwendigkeit und Verhältnismäßigkeit der in Kapitel 4 aufgeführten ETIAS-Datenverarbeitungstätigkeiten zu bewerten.

Anstatt jedoch das technische Konzept und die Funktionen zu bewerten, die eu-LISA zur Umsetzung der ETIAS-Verordnung gewählt hat, wird in Kapitel 6 hauptsächlich die ETIAS-Verordnung bewertet. Der EDSB weist nachdrücklich darauf hin, dass eine solche Bewertung in die Zuständigkeit des Gesetzgebers und nicht von eu-LISA fällt.

Eu-LISA hat sich an die erlassenen Rechtsvorschriften zu halten und sie umzusetzen. Die von eu-LISA als Verantwortliche durchzuführende DSFA betrifft ihre Entscheidungen bezüglich der technischen Gestaltung.[26]
Sie sollte versuchen, folgende Frage zu beantworten: „Wie kann eu-LISA ihre vom Gesetzgeber übertragenen Aufgaben auf vorschriftsmäßige und datenschutzfreundliche Weise erfüllen?“

Wenn beispielsweise der Antragsentwurf eingereicht und gespeichert wird, erhebt das System vom Nutzer (Drittstaatsangehöriger) Informationen wie IP-Adresse, Zeitstempel und Geräteinformationen (Abschnitt 5.3.10). Dies könnte zu Protokollierungs-, Prüfungs- und

[26] Siehe EDSB, Toolkit zur Rechenschaftspflicht, Teil I, S. 7f.

Statistikzwecken im Browser des Nutzers geschehen (um sicherzustellen, dass angemessene Statistiken über die zu unterstützenden Browser bereitgestellt werden).

Eu-LISA sollte die Notwendigkeit und Verhältnismäßigkeit aller in diesem Zusammenhang erhobenen Daten bewerten. Sie sollte sicherstellen, dass nur die für das Gerät des Nutzers erforderlichen Daten erhoben werden und dass es eine angemessene Strategie gibt, diese Informationen nicht an andere Stellen (z. B. Strafverfolgungsbehörden) weiterzugeben, wenn dies nicht im Zusammenhang mit der Ermittlung in der Frage steht, wer einen Antrag für eine andere Person oder auf Nichtabweisung gestellt hat. Das Risiko, dass nur die erforderlichen Daten nicht ermittelt und verarbeitet werden, könnte dazu führen, dass der Nutzer einem Profiling oder einer unbefugten Nutzung solcher Informationen unterzogen wird.

Ein weiteres Beispiel könnte der Einsatz spezifischer Instrumente sein. Unter bestimmten Bedingungen ist es dem Antragsteller gestattet, die erforderliche Befragung per Fernkommunikation durchzuführen.[27] Der Bedienstete der nationalen ETIAS-Stelle und der Drittstaatsangehörige einigen sich anhand einer von eu-LISA vorab erstellten Liste auf das einzusetzende Instrument. Wenn beim Einsatz des Befragungsinstruments mehr personenbezogene Daten über den Drittstaatsangehörigen erhoben werden als notwendig (z. B. Verbindungsdaten), besteht die Gefahr des Profiling und der unbefugten Nutzung dieser Daten.

Die Zuständigkeit von eu-LISA umfasst die Analyse der personenbezogenen Daten, die diese vorab ausgewählten Tools über die Drittstaatsangehörigen erheben, und ihrer Geräte, sowie die Beantwortung der Frage, ob diese die Mindestanforderungen erfüllen, um das Ziel der Befragung zu erreichen. Ferner sollte jede Übermittlung personenbezogener Daten (Inhalt der Kommunikation oder Metadaten) an Dritte und Drittländer im Hinblick auf die Rechtmäßigkeit, aber auch auf die Notwendigkeit und Verhältnismäßigkeit eingehend geprüft werden.

Der EDSB empfiehlt, Kapitel 6 zu überarbeiten und zu erläutern,

[27] Artikel 27 Absatz 4 der ETIAS-Verordnung bestimmt: „Befindet sich das dem Wohnort des Antragstellers am nächsten gelegene Konsulat in einer Entfernung von mehr als 500 km, so wird dem Antragsteller die Möglichkeit geboten, dass die Befragung mit Mitteln der Audio- und Videofernkommunikation durchgeführt wird. Beträgt die Entfernung weniger als 500 km, so können sich der Antragsteller und die nationale ETIAS-Stelle des zuständigen Mitgliedstaats darauf einigen, solche Audio- und Videokommunikationsmittel zu benutzen."

- warum die vorgeschlagene Gestaltung und die technischen Funktionen des ETIAS wirksame Mittel zur Umsetzung der ETIAS-Verordnung darstellen,
- ob eu-LISA Alternativen geprüft hat, und
- warum die gewählten Lösungen aus der Grundrechtsperspektive das am wenigsten in die Privatsphäre eingreifende Mittel sind.

3.7. Risikoanalyse und Festlegung der im Hinblick auf die festgestellten Risiken ergriffenen Kontrollen

Ein „Risiko" in diesem Sinne ist ein mögliches Ereignis, das Schäden oder Verluste verursachen oder die Fähigkeit, die Ziele zu erreichen, beeinträchtigen könnte. Bei der Definition eines Risikos im Zusammenhang mit einer DSFA besteht das Ziel darin, die Grundrechte und -freiheiten der betroffenen Personen zu schützen und/oder die Datenschutzgrundsätze des geltenden Rechtsrahmens einzuhalten (mit denen ebenfalls die Rechte betroffener Personen geschützt werden sollen). Auch wenn ein Compliance-Risiko für die Organisation besteht, liegt der Schwerpunkt auf den Auswirkungen auf die Rechte und Freiheiten der betroffenen Personen.[28]

Wie bereits dargelegt (Ziffern 3.4 und 3.5), ist die in der DSFA für das System und die Datenverarbeitung enthaltene Beschreibung einem klaren Konzept des gesamten Systems nicht zuträglich, das erforderlich ist, um hohe Risiken zu ermitteln und die möglichen Auswirkungen auf die betroffenen Personen (Drittstaatsangehörige) zu verstehen.

Die Risikobewertung in einer DSFA befasst sich mit folgenden Fragen[29]:

- was könnte schief gehen (Risiko),
- was könnte dazu führen, dass das Risiko eintritt (Quelle),
- wie wahrscheinlich ist es, dass das Risiko Personen schaden könnte (Wahrscheinlichkeit),
- welche nachteiligen Auswirkungen würde es für Personen geben (Auswirkungen),

[28] Siehe EDSB, Toolkit zur Rechenschaftspflicht, Teil II, S. 8ff.

[29] Siehe WP29, „Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt", angenommen vom EDSA am 4. April 2017, abrufbar unter: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/data-protection-impact-assessments-high-risk-processing_en , S. 17 und 22.

- wie schwerwiegend wären die nachteiligen Auswirkungen (Schwere),
- welche Kontrollmaßnahmen wären geeignet, die Risiken zu beseitigen, zu verringern oder zu minimieren (Eindämmungsmaßnahmen).

In Kapitel 7 (S. 120) sind die in Kapitel 5 identifizierten Risiken aufgeführt, in dem die Funktionalität beschrieben wird (z. B. Risiko 1 auf S. 60). Der EDSB stellt fest, dass die meisten Risiken damit zusammenhängen, dass bei der Verarbeitung falsch vorgegangen wird (z. B. unbefugter Zugang zu privaten Daten in Risiko 1), oder dass gegen einen Datenschutzgrundsatz (z. B. Treu und Glauben, Transparenz, Richtigkeit, Sicherheit in Risiko 1) verstoßen wird. Auf die Auswirkungen auf die betroffene Person wird jedoch nicht eingegangen. Der EDSB betont, wie wichtig es ist, alle vier Elemente zu beschreiben, d. h. die Quelle, das Risiko, die Auswirkungen und die Risikoeindämmungsmaßnahme(n), um eine ordnungsgemäße Risikobewertung zu ermöglichen.

Nachstehend für Risiko 1 ein Beispiel für die erwarteten Elemente:

- Quelle: fehlerhafte E-Mail-Eingabe der betroffenen Person.
- Risiko: unbefugter Zugang – Die unbefugte Person, die auf den Antrag zugreift, kann den Antrag zurückziehen, die Informationen anderen Personen mitteilen oder die Informationen für andere Zwecke verwenden.
- Auswirkungen: finanzielle Folgen, Auswirkungen auf den Ruf, Identitätsdiebstahl.
- Eindämmung: Validierung der E-Mail, bevor der Nutzer personenbezogene Daten eingibt.

Der EDSB hält fest, dass die DSFA eine Wissensbasis für Wirkungsbewertungen enthält, in der Beispiele für physische, materielle und moralische Auswirkungen auf die Person aufgeführt sind. Er schlägt vor, die Auswirkungen der einzelnen Risiken auf der Grundlage dieser Wissensbasis zu beschreiben.

Darüber hinaus stellt der EDSB fest, dass in der DSFA 21 Risiken aufgeführt sind, die nach Auffassung von eu-LISA nach Anwendung der Maßnahmen zur Risikoeindämmung begrenzt oder vernachlässigbar sind. Diese Liste enthält jedoch keine Risiken, die nach ihrer Eindämmung durch die grundlegenden Sicherheitsmaßnahmen von eu-LISA als beseitigt oder gering eingestuft wurden. Der EDSB betont, dass solche Risiken und die Maßnahmen zu ihrer Eindämmung in der DSFA als Nachweis dafür dargelegt werden sollten, dass alle relevanten Risiken ermittelt wurden, aber als eindämmbar gelten. Eine solche

Vorgehensweise würde auch als Richtschnur für die Einbeziehung dieser Maßnahmen in das Konzept für die Umsetzung des ETIAS-Systems in den nächsten Phasen dienen.

Darüber hinaus stellt der EDSB fest, dass die Sicherheitsanalyse (Abschnitt 7.1.7) unvollständig ist, da noch keine Bewertung der Sicherheitsrisiken für ETIAS durchgeführt wird. Da der Prozess des Informationssicherheitsmanagements eine Bewertung des Sicherheitsrisikos für die Vermögenswerte der Organisation (einschließlich personenbezogener Daten) mit Schwerpunkt auf der Organisation umfasst, wird jede Entscheidung über die Durchführung von Eindämmungsmaßnahmen auf der Grundlage der Kosten für und der Auswirkungen auf die Organisation getroffen.

Das Ergebnis der Bewertung der Sicherheitsrisiken (Restrisiken nach Risikoeindämmungsmaßnahmen) sollte in die DSFA einfließen, um das Risiko auch aus der Sicht der betroffenen Personen zu bewerten. Zwar wäre eine analytische Erläuterung der Sicherheitsrisiken (z. B. nach Art des Angriffs böswilliger Nutzer) nicht erforderlich, doch sollte eine allgemeine Beschreibung dieser Risiken vorgelegt werden (z. B. böswillige externe Akteure, die sich über die Website unberechtigten Zugang zu den Daten des Antragstellers verschaffen), die den Datenschutzrisiken (z. B. unbefugter Zugang) zugeordnet und neu bewertet werden.

Der EDSB begrüßt, dass eu-LISA im Rahmen der DSFA bereits einige Sicherheitsrisiken ermittelt hat (z. B. [....]). Sie hat auch im Voraus spezifische Sicherheitsrisiken ermittelt, die erhebliche Auswirkungen auf personenbezogene Daten haben werden, und zwar durch die Annahme von Schwachstellen von [...].

Der EDSB stellt jedoch fest, dass keine Risiken im Zusammenhang mit Sicherheitsvorfällen in der ETIAS-Zentralstelle ermittelt wurden. Er erinnert daran, dass eu-LISA in Bezug auf das Informationssicherheitsmanagement des ETIAS-Zentralsystems als Verantwortlicher fungiert, und erwartet eine gründliche Bewertung der Datenschutzrisiken, die aus Risiken für die Informationssicherheit erwachsen.

Insgesamt sollten beispielhaft folgende Risiken betrachtet werden:

- Risiken im Zusammenhang mit dem unbefugten Zugriff auf den eingereichten Antrag, z. B. durch

- eine andere Person, die auf die E-Mail des Nutzers zugreift und Zugang zum Link des Antrags erhält und dann den Antrag zurückzieht oder bearbeitet;
- einen technischer Fehler des Systems, das den Link an einen anderen Antragsteller versendet;
- einen Nutzer, der sich bei seiner E-Mail-Adresse verschreibt, sodass der Hyperlink des Antrags an eine andere E-Mail-Adresse geht;.
- einen Nutzer, der irrtümlich glaubt, dass durch das Speichern des Antragsentwurfs sein Antrag eingereicht wird;
- einen Nutzer, der den Zugang zum E-Mail-Konto verliert, oder dessen E-Mail-Anbieter seinen Betrieb einstellt.

- Risiken im Zusammenhang mit der automatisierten Bearbeitung des Antrags (einschließlich des Managements der Überwachungsliste), z. B. die Übermittlung der Daten des Antragstellers an Europol aufgrund
  - eines TREFFERS mit Europol-Daten, wenn der Antragsteller als Opfer oder Zeuge registriert ist;
  - eines falsch positiven TREFFERS, der das Ergebnis einer fehlerhaften technischen Umsetzung der Risikoindikatoren nach Artikel 33 ist (Unterabschnitt 5.5.1);
  - einer nicht aktualisierten Überwachungsliste (Abschnitt 5.9.5).

- Risiken im Zusammenhang mit der Zahlung der ETIAS-Antragsgebühr, z. B. aufgrund
  - eines Missbrauchs der Zahlungsdaten durch die Bank des Antragstellers (sie weiß, dass der Karteninhaber beim ETIAS eine Gebühr bezahlt hat, kennt aber keine Einzelheiten des Antrags);
  - eines technischen Problems, das dazu führt, dass die Zahlungsbestätigung ausbleibt.

- Risiken im Zusammenhang mit dem Zugang von Strafverfolgungs- oder Grenzkontrollbehörden, z. B. aufgrund
  - der Ermittlung eines falschen Treffers anhand der Ergebnisse der Eingabe der Daten der Antragsteller in die LEA-Systeme;
  - einer umfassenden Abfrage des Systems, ohne dass die Kriterien für eine Abfrage erfüllt sind (schwere Kriminalität, der Antragsteller befindet sich an der Grenze, im EES sind bereits Informationen vorhanden usw.),
  - der Speicherung und Nutzung abgefragter Daten für andere Zwecke.

- Risiken im Zusammenhang mit dem Zugang der nationalen ETIAS-Stellen zum ETIAS-Zentralsystem:
    - unbefugte Datenexporte durch nationale ETIAS-Stellen von im ETIAS-Zentralsystem gespeicherten Daten und Import dieser Daten in nationale Systeme für andere Verarbeitungszwecke.

- Risiken im Zusammenhang mit dem Zugang von Beförderern, z. B. aufgrund
    - der Suche nach Antragstellern, die die Reise nicht antreten;
    - des Zugriffs auf nicht aktuelle Daten in der schreibgeschützten Datenbank (in den letzten 24 Stunden wurde eine ETIAS ausgestellt).

- Risiken im Zusammenhang mit der Ausübung des Auskunftsrechts betroffener Personen, z. B. aufgrund
    - einer nicht ordnungsgemäßen Überprüfung der Identität eines Antragstellers, der einen Antrag auf Auskunft/Berichtigung/Löschung stellt;
    - der Unmöglichkeit, die Behörde, die den Antragsteller betreffende Daten in eines der vom ETIAS-Zentralsystem abgefragten Systeme eingibt, eindeutig zu identifizieren.

- Risiken im Zusammenhang mit Datensicherheitsvorfällen oder der Datenspeicherung, z. B. aufgrund
    - eines Versäumnisses, die betroffene Person über eine Verletzung des Schutzes personenbezogener Daten zu informieren (wenn entweder auf ihre Daten zugegriffen wird oder sie geändert oder gelöscht werden);
    - der unterbliebenen Löschung von Daten aus Anträgen oder Protokollen gemäß den Vorgaben für die Datenspeicherung;
    - der nicht erfolgten Zusammenführung von Protokollen aus verschiedenen Systemen zur Untersuchung eines Sicherheitsvorfalls wie unbefugter Zugriff.

Vor diesem Hintergrund empfiehlt der EDSB Folgendes:

- Überprüfung der DSFA, sobald die Gesamtbeschreibung der Datenströme im System vollständig ist, um sicherzustellen, dass keine hohen Risiken außer Acht gelassen werden.

- Gewährleistung, dass für jedes ermittelte spezifische Risiko die Quelle, die Auswirkungen und die Maßnahme zu seiner Eindämmung beschrieben werden.
- Auflistung *aller* ermittelten Risiken, einschließlich geringer Risiken.
- Überarbeitung der DSFA und Neubewertung der Datenschutzrisiken auf der Grundlage der nach der ETIAS-Sicherheitsrisikobewertung ermittelten Sicherheitsrisiken.

4. SCHLUSSFOLGERUNGEN

Der EDSB begrüßt, dass die DSFA in ihrem Aufbau generell dem Muster der im „Toolkit zur Rechenschaftspflicht" des EDSB bereitgestellten DSFA entspricht. Angesichts der Komplexität des ETIAS begrüßt er ferner den Top-down-Ansatz des Berichts (d. h. eine Beschreibung des Gesamtbilds mit den wichtigsten Verarbeitungsvorgängen und anschließend eine detailliertere und spezifischere Beschreibung dieser Vorgänge).

Als „lebendes Instrument" muss die DSFA nicht in Stein gemeißelt sein, sondern kann während der Umsetzung und des Betriebs des ETIAS weiter vervollständigt und weiterentwickelt werden. Die vorstehende Analyse hat jedoch gezeigt, dass in dieser frühen Umsetzungsphase noch wichtige Elemente fehlen oder nicht klar und umfassend genug dargestellt werden, um eine ordnungsgemäße und umfassende Ermittlung und Bewertung der Risiken für die Grundrechte des Einzelnen zu ermöglichen.

Angesichts der Komplexität des ETIAS-Systems einschließlich - unter anderem - seiner Verknüpfungen mit anderen Systemen und der Schlüsselrolle mehrerer Interessenträger empfiehlt der EDSB eu-LISA, vor der Einführung des Systems eine umfassende Version der DSFA auszuarbeiten, die auch die von anderen für die Verarbeitung Verantwortlichen in ihren eigenen Datenschutz-Risikobewertungen ermittelten Risiken und Risikoeindämmungsmaßnahmen umfasst. Dadurch kann sichergestellt werden, dass die Risiken, die sich insgesamt aus der Nutzung des ETIAS ergeben, angemessen bewältigt werden.

Der EDSB spricht gegenüber eu-LISA die folgenden Empfehlungen aus, mit denen die Einhaltung der ETIAS-Verordnung (insbesondere in Bezug auf die Umsetzung des Grundsatzes des Datenschutzes durch Technikgestaltung und datenschutzfreundliche Voreinstellungen) und der Verordnung sichergestellt werden soll:

- Angabe und Beschreibung aller anwendbaren Kriterien, die zu der Entscheidung über die Durchführung einer DSFA führen.

- Vor der Inbetriebnahme des ETIAS Vorlage einer umfassenden DSFA, die auch die Risiken behandelt, die in den DSFA der anderen Interessenträger (d. h. der ETIAS-Zentralstelle, der nationalen ETIAS-Stellen und/oder von Europol) ermittelt wurden.

- Aufnahme in die DSFA von Risiken im Zusammenhang mit den Interaktionen des Systems mit Verarbeitungsvorgängen unter der Verantwortung anderer Interessenträger (d. h. der ETIAS-Zentralstelle, der nationalen ETIAS-Stellen und/oder Europols) in enger Abstimmung mit diesen Stellen.

- Hinzufügung in Kapitel 4 der DSFA von zwei Datenflussdiagrammen („Ebene 0" und „erste Ebene"), um eine klare Visualisierung der Art und Weise zu ermöglichen, wie Informationen im Allgemeinen in das System eingegeben und daraus gelöscht werden, welche Änderungen sie erfahren und wo die Informationen gespeichert werden. Das erste Diagramm würde das System, die externen Stellen, mit denen es interagiert, und die Datenströme zwischen dem System und den externen Stellen aufzeigen. Das zweite Diagramm wäre eine Erweiterung des ersten und würde die wichtigsten Datenverarbeitungsvorgänge umfassen.

- In Kapitel 5 sollte sichergestellt werden, dass
  - für jeden Hauptdatenverarbeitungsvorgang ein Flussdiagramm, eine Tabelle und eine Beschreibung beigefügt sind,
  - alle Schritte im Flussdiagramm und in der Tabelle aufgeführt und klar und einheitlich beschrieben sind,
  - die Beschreibung jedes einzelnen Schritts den Nutzer, die Maßnahme, die Daten und den Datenträger umfasst.

- In Kapitel 6 sollte erläutert werden,
  - warum die vorgeschlagene Gestaltung und die technischen Funktionen des ETIAS wirksame Mittel zur Umsetzung der ETIAS-Verordnung darstellen,
  - ob eu-LISA Alternativen geprüft hat, und
  - warum die gewählten Lösungen aus der Grundrechtsperspektive das am wenigsten in die Privatsphäre eingreifende Mittel sind.

– Überarbeitung der DSFA, sobald die Gesamtbeschreibung der Datenströme im System vollständig ist, um sicherzustellen, dass keine hohen Risiken außer Acht gelassen werden.

– Gewährleistung, dass für jedes ermittelte spezifische Risiko die Quelle, die Auswirkungen und die Maßnahme zu seiner Eindämmung beschrieben werden.

– Auflistung *aller* ermittelten Risiken, einschließlich geringer Risiken.

– Überarbeitung der SDFA nach der Bewertung des ETIAS-Sicherheitsrisikos.

Geschehen zu Brüssel am *

Wojciech Rafał WIEWIÓROWSKI
(elektronisch unterzeichnet)