Stellungnahme auf Ersuchen der Europäischen Staatsanwaltschaft um vorherige Konsultation zu den in der Datenschutz-Folgenabschätzung zu ihrem Fallbearbeitungssystem festgestellten Risiken

1. VERFAHREN

Am 24. Juli 2020 ging dem Europäischen Datenschutzbeauftragten (EDSB) ein Ersuchen um vorherige Konsultation gemäß Artikel 72 Absatz 1 Buchstabe a der Verordnung (EU) 2017/1939 vom 12. Oktober 2017[1] (im Folgenden: EUStA-Verordnung) zu, das die gemäß Artikel 71 der EUStA-Verordnung durchgeführte Datenschutz-Folgenabschätzung (im Folgenden: DSFA) zu ihrem Fallbearbeitungssystem betraf.

Die von der Europäischen Staatsanwaltschaft (im Folgenden: EUStA) zugesandte Meldung enthielt eine Beschreibung der Verarbeitungsumgebung, eine Bewertung der Notwendigkeit und Verhältnismäßigkeit sowie eine Risikoanalyse und Angaben zur Risikoeindämmung.[2] Von der EUStA wurden zusammen mit der DSFA folgende Unterlagen eingereicht:

[AUSLASSUNG]

Der EDSB begrüßt den Umstand, dass die EUStA, wie im Ergebnis der DSFA erwähnt, die Datenschutzanforderungen im Zuge der Umsetzungs- und Gestaltungsphase des Fallbearbeitungssystems ([AUSLASSUNG]) berücksichtigt hat.

Gemäß Artikel 72 Absatz 4 der EUStA-Verordnung unterbreitet der EDSB seine Stellungnahme innerhalb eines Zeitraums von bis zu sechs Wochen nach Erhalt des Ersuchens um Konsultation, wobei diese Frist um einen weiteren Monat verlängert werden kann. Die Meldung ging am 24. Juli 2020 ein. Unter Berücksichtigung der Komplexität der geplanten Verarbeitung teilte der EDSB der EUStA am 18. August 2020 die Verlängerung der Frist um einen Monat mit. Der EDSB muss seine Stellungnahme also bis zum **5. Oktober 2020** abgeben.

2. BESCHREIBUNG DER VERARBEITUNG

[1] ABl. L 283 vom 31.10.2017, S. 1-71.

[2] Artikel 71 Absatz 2 der EUStA-Verordnung bestimmt: „Die Folgenabschätzung gemäß Absatz 1 trägt den Rechten und den berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung und enthält zumindest eine **allgemeine Beschreibung der geplanten Verarbeitungsvorgänge** und eine **Bewertung der** in Bezug auf die Rechte und Freiheiten der betroffenen Personen bestehenden **Risiken** sowie der **geplanten Abhilfemaßnahmen**, **Garantien**, **Sicherheitsvorkehrungen** und **Verfahren**, durch die der Schutz operativer personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird."

Postanschrift: Rue Wiertz 60 – 1047 Brüssel, Belgien
Dienststelle: Rue Montoyer 30 – 1000 Brüssel, Belgien
E-Mail: edps@edps.europa.eu – Website: www.edps.europa.eu
Tel.: +32 2283-1900 – Fax: +32 2283-1950

Die EUStA wurde durch die EUStA-Verordnung mit der Befugnis zur strafrechtlichen Untersuchung und Verfolgung sowie der Anklageerhebung in Bezug auf Straftaten zum Nachteil des Haushalts der Union wie Betrug, Korruption und schweren grenzüberschreitenden Mehrwertsteuerbetrug errichtet.

Als Agentur der Union, die Tätigkeiten wahrnimmt, die in den Anwendungsbereich von Kapitel 4 bzw. Kapitel 5 Titel V des Dritten Teils des AEUV fallen, verarbeitet die EUStA operative personenbezogene Daten im Einklang mit den Bestimmungen der EUStA-Verordnung und ihrer eigenen Geschäftsordnung. Die operativen personenbezogenen Daten werden gemäß Artikel 44 der EUStA-Verordnung in einem Fallbearbeitungssystem (nach der englischen Bezeichnung auch als CMS abgekürzt) verarbeitet.

Das Fallbearbeitungssystem der EUStA ist gemäß Artikel 44 der EUStA-Verordnung eingerichtet, der vorsieht, dass es gemäß den Vorschriften der EUStA-Verordnung und der Geschäftsordnung der EUStA verwaltet wird. Gemäß Artikel 44 Absatz 4 der EUStA-Verordnung enthält das Fallbearbeitungssystem ein Register der Informationen, die von der EUStA gemäß Artikel 24 erlangt wurden; einen Index aller Verfahrensakten; und alle Informationen aus den Verfahrensakten, die elektronisch gespeichert sind. Die EUStA hat die Absicht, ihr Fallbearbeitungssystem in den nächsten Monaten in Betrieb zu nehmen.

3. RECHTLICHE UND TECHNISCHE BEWERTUNG

3.1. Erfordernis der vorherigen Konsultation gemäß Artikel 72 der EUStA-Verordnung

Nach Artikel 72 der EUStA-Verordnung ist bezüglich der Verarbeitung in neu anzulegenden Dateisystemen vorab der EDSB zu konsultieren, wenn

a) aus einer Datenschutz-Folgenabschätzung gemäß Artikel 71 hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern die EUStA keine Maßnahmen zur Eindämmung des Risikos trifft, oder
b) die Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, Mechanismen oder Verfahren, ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen zur Folge hat.

Aus der DSFA[3] geht hervor, dass die Verarbeitung operativer Daten im Fallbearbeitungssystem Strafverfolgungs- und justiziellen Zwecken dient, so dass es sich per definitionem um einen Verarbeitungsvorgang handelt, dem ein hohes Risiko für die betroffenen Personen innewohnt. Darüber hinaus lässt die DSFA erkennen, dass – mangels von der EUStA ergriffener Maßnahmen zur Risikoeindämmung – hohe Risiken bestehen. Somit ist gemäß Artikel 72 Absatz 1 Buchstabe a der EUStA-Verordnung die Verpflichtung der EUStA gegeben, den EDSB vorab zu konsultieren. Darüber hinaus ist die vorherige Konsultation auch gemäß Artikel 71 Absatz 1 Buchstabe b erforderlich, da diese Art der Verarbeitung, für die neue Mechanismen und Verfahren Anwendung finden, per se ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen zur Folge hat, sowohl wegen der Art der verarbeiteten Daten als auch wegen ihrer potenziellen Auswirkungen auf das Recht der betroffenen Personen auf Datenschutz und andere Grundrechte, etwa das Recht auf Diskriminierungsfreiheit, das

[3] Seite 5.

Recht auf einen wirksamen Rechtsbehelf und ein faires Verfahren, die Unschuldsvermutung und das Verteidigungsrecht.

3.2. Gegenstand der Stellungnahme

Die Stellungnahme des EDSB im Rahmen dieser vorherigen Konsultation **betrifft nur die DSFA, so wie diese in der Meldung** vom 24. Juli 2020 (V4.0) einschließlich der in der Anlage beigefügten Unterlagen **beschrieben ist**.

Diese Stellungnahme konzentriert sich auf die Hauptaspekte, die hinsichtlich der Einhaltung des einschlägigen Rechtsrahmens für den Datenschutz problematisch sind oder aus anderen Gründen weitere Prüfung verdienen.

Der EDSB wird zum jetzigen Zeitpunkt keine spezifischen Bemerkungen zu den mit der DSFA eingereichten Unterlagen machen. Der EDSB hat bereits zur Geschäftsordnung der EUStA [EDSB Sache: 2020-0781] und zu den Regeln der EUStA für die Verarbeitung personenbezogener Daten [EDSB Sache: 2020-0782] Anmerkungen gemacht und Empfehlungen gegeben.[4] Weitere Ersuchen der EUStA um Konsultation sind dem EDSB willkommen.

Der EDSB merkt an, dass die DSFA keine Bestimmungen über den Zugriff von Eurojust und OLAF auf Informationen im Fallbearbeitungssystem der EUStA auf Grundlage eines Treffer/Kein-Treffer-Verfahrens (wie in den Artikeln 100 Absatz 3 und 101 Absatz 5 der EUStA-Verordnung vorgesehen) enthält. Sollte die EUStA einen solchen Dienst in ihrem Fallbearbeitungssystem implementieren, würde der EDSB erwarten, gemäß Artikel 72 der EUStA-Verordnung konsultiert zu werden.

Der EDSB erwartet auch, zu allen wichtigen Überarbeitungen der DSFA, die wegen erheblicher Abänderung der personenbezogene Daten betreffenden Verarbeitungsvorgänge im Fallbearbeitungssystem erfolgen, konsultiert zu werden.

3.3. Rechtsgrundlage der Verarbeitung

Der Verarbeitungszweck fällt unter **Artikel 44** der EUStA-Verordnung, der vorsieht, dass die EUStA ein Fallbearbeitungssystem einrichtet, dessen Zweck es ist,

a) die Verwaltung der Ermittlungen und Strafverfolgungsmaßnahmen der EUStA zu unterstützen;
b) den sicheren Zugang zu Informationen über Ermittlungen und Strafverfolgungsmaßnahmen bei der zentralen Dienststelle und durch die Delegierten Europäischen Staatsanwälte zu gewährleisten;

[4] Vgl. Schreiben des Europäischen Datenschutzbeauftragten an den Europäischen Generalstaatsanwalt vom 17. September 2020 und die in der Anlage beigefügten Kommentare.

c) den Abgleich von Informationen und die Extraktion von Daten für operative Analysen und statistische Zwecke zu ermöglichen;
d) die Überwachung zu erleichtern, um sicherzustellen, dass die Verarbeitung operativer personenbezogener Daten rechtmäßig ist und mit den einschlägigen Bestimmungen dieser Verordnung im Einklang steht.

3.4. Bewertung der DSFA

Von der EUStA wurde eine Reihe von Risiken für betroffene Personen festgestellt. Laut der DSFA umfassen die Maßnahmen zur Eindämmung der festgestellten Risiken technische (Vorgaben für die Gestaltung und Struktur des Fallbearbeitungssystems), organisatorische bzw. rechtliche Maßnahmen (rechtsverbindliche Durchführungsregeln innerhalb der EUStA, z. B. Geschäftsordnung, interne Vorschriften für die Verarbeitung personenbezogener Daten, interne Vorschriften für den Schutz von nicht als Verschlusssache eingestuften sensiblen Informationen).

Die EUStA kam zu dem Ergebnis, dass „die vorhandenen Maßnahmen organisatorischer, technischer oder rechtlicher Art die Rest- und Gesamtrisiken auf ein Maß reduzieren, das für die EUStA hinnehmbar ist und in angemessenem Verhältnis zu dem mit den Verarbeitungsvorgängen verfolgten Ziel steht …“.[5]

Als Erstes möchte der EDSB hervorheben, dass die Qualität der DSFA hervorragend war, was die angewandte Methodologie (einschließlich der Risikofaktoren und der Matrix zu Wahrscheinlichkeit und Auswirkungen) wie auch den Inhalt (Situationsbeschreibung und Analyse, insbesondere im Hinblick auf die betroffenen Personen, die das jeweilige Risiko hauptsächlich betrifft) angeht. Der EDSB schätzt insbesondere, dass die EUStA ihre Analyse auf die Risiken für die betroffenen Personen konzentriert hat.

Der EDSB wird im Folgenden auf die **wichtigsten Datenschutzprobleme** eingehen, die die hier in Rede stehende Verarbeitung personenbezogener Daten betreffen, unter Berücksichtigung der von der EUStA vorgesehenen Maßnahmen, die den Datenschutzrisiken entgegenwirken sollen. Des Weiteren wird auch auf die Auswirkungen auf **sonstige Grundrechte** der betroffenen Personen eingegangen werden. Der EDSB nimmt zur Kenntnis, dass die EUStA bei der Feststellung und Beschreibung der Risiken auch Risiken für andere Grundrechte als das Recht auf Datenschutz berücksichtigt hat (ohne diese allerdings ausdrücklich zu benennen).

Trotz der guten Gesamtqualität der DSFA hat der EDSB einige spezifische Anmerkungen und Empfehlungen zur Methodologie (Abschnitt 3.4.1) und zu den von der EUStA festgestellten Risiken (Abschnitt 3.4.2).

[5] Seite 5.

3.4.1. DSFA-Methode

a) **Keine Unterscheidung zwischen „Ereignissen“ und „Risiken“**

Die DSFA enthält eine Spalte mit der Überschrift „**Ereignis/Risiko**“. „Ereignis“ und „Risiko“ sind jedoch zwei verschiedene Begriffe: Ein „Ereignis“ ist ein Geschehen, das Auswirkungen und eine Wahrscheinlichkeit hat, wohingegen sich ein „Risiko“ aus einem Ereignis und einer möglichen (vor allem negativen) Folge eines Ereignisses ergibt. Die in dem Dokument verwendete Terminologie sollte entsprechend angepasst werden, um sicherzustellen, dass Ereignisse und Risiken nicht vermischt werden (die Spalte 2 in Tabelle 7.2. der DSFA sollte ausschließlich mit „Ereignisse“ überschrieben sein). Des Weiteren sollte der Inhalt der Spalte 4 („Risiko für die betroffene Person“) in Tabelle 7.2 der DSFA ausschließlich die mit dem jeweiligen Ereignis verbundenen Risiken beschreiben und nichts anderes enthalten.

Empfehlung 1: Anpassung der DSFA, um dem begrifflichen Unterschied zwischen „Ereignissen“ und „Risiken“ Rechnung zu tragen.

b) **Allgemein unzureichende Beschreibung der Eindämmungsmaßnahmen**

In der DSFA sind die Eindämmungsmaßnahmen zumeist recht abstrakt formuliert, so dass nicht konkret angegeben ist, wie dem festgestellten Risiko entgegengewirkt werden wird und welche konkreten Eindämmungsmaßnahmen gegen spezifische Risiken ergriffen werden. Dies ist zum Teil auf das vorgenannte Problem bezüglich „Ereignissen“ und „Risiken“ zurückzuführen, aber auch darauf, dass in der Analyse zuweilen nicht angegeben ist, wie das Risiko sich verwirklichen kann, so dass die Eindämmungsmaßnahme nicht hinreichend spezifisch angegeben werden kann. Obwohl die internen Vorschriften der EUStA (z. B. die Geschäftsordnung, die Internen Regeln für die Verarbeitung personenbezogener Daten oder die Regeln für den Datenschutzbeauftragten) unter Umständen durchaus spezifische Regeln enthalten, ist häufig unklar, welche spezifische Bestimmung der vorgenannten Vorschriften im Einzelfall gilt und mit welchen konkreten Maßnahmen das Risiko eingedämmt werden wird.

So bezieht sich das im DSFA festgestellte **Risiko Nr. 34** darauf, dass „**keine ordnungsgemäße Meldung und Reaktion auf Verletzungen des Schutzes personenbezogener Daten**“ erfolgt. Als Eindämmungsmaßnahmen sind „Vorschriften über die Verarbeitung personenbezogener Daten, Geschäftsordnung, Einbeziehung und Konsultation des DSB“ angegeben.

Empfehlung 2: Soweit noch nicht geschehen, sollten Angaben zu spezifischen Maßnahmen zur Eindämmung des betreffenden Risikos (etwa technische und organisatorische Maßnahmen, wobei, soweit dies im Fallbearbeitungssystem implementiert ist, bei der Eindämmungsmaßnahme die Funktionalität beschrieben sein sollte) sowie Verweise auf die einschlägigen internen Vorschriften in den jeweiligen Abschnitt mit den Eindämmungsmaßnahmen für jedes der festgestellten Risiken aufgenommen werden.

Empfehlung 3: Für die ordnungsgemäße Meldung von Verletzungen des Schutzes personenbezogener Daten und ggf. Benachrichtigung darüber sowie für das Ergreifen entsprechender Maßnahmen zur Eindämmung der Risiken für die betroffenen Personen sind

Grundsätze für den Fall der Verletzung des Schutzes personenbezogener Daten zu entwerfen und aufzustellen, in denen die Hauptaspekte (etwa die Rollen und Funktionen, die einzubeziehen sind, wenn es zu Sicherheitsvorfällen oder Verletzungen des Schutzes personenbezogener Daten kommt), die Risikobewertung, die Verfahren zur Meldung an den EDSB sowie ggf. die Benachrichtigung der betroffenen Personen und angemessene Eindämmungsmaßnahmen geregelt sind.

c) **Überschrift der Spalte „Zugrunde liegende Datenschutzgrundsätze" reflektiert nicht ihren Inhalt**

Der Inhalt der Spalte „Zugrunde liegende Datenschutzgrundsätze" in Tabelle 7.2 bezieht sich nicht nur auf Datenschutzgrundsätze, welche, in engen Sinne, die in Artikel 47 der EUStA-Verordnung aufgeführten Grundsätze sind. In der Spalte geht es z. B. auch um die Ausübung der Rechte der betroffenen Personen, die Benachrichtigung über Datenschutzverletzungen und Übermittlungen, d. h. um allgemeine Datenschutzvorschriften.

Empfehlung 4: Anpassung der Überschrift der vorgenannten Spalte, so dass klar wird, dass sich diese auf allgemeine Datenschutzvorschriften bezieht.

d) **Fehlen wichtiger Aspekte bezüglich der Überprüfung der DSFA**

[AUSLASSUNG]

Trotz des Erfordernisses, die Datenschutz-Folgenabschätzung unter bestimmten Umständen zu überprüfen, enthält die DSFA weder Angaben dazu, in welchen Abständen die regelmäßige Überprüfung durchzuführen ist, noch zu den Kriterien für die Vornahme außerordentlicher Überprüfungen oder zu den Stellen, die für die Überprüfung verantwortlich sind.

Empfehlung 5: Aufnahme einer Angabe dazu, in welchen **Abständen die Überprüfung der DSFA** nach Inbetriebnahme des Fallbearbeitungssystems erfolgt. Im Hinblick auf die vorstehenden Erwägungen empfiehlt der EDSB, die DSFA jährlich sowie bei jeder bedeutenden Entwicklung, die Auswirkungen auf die DSFA hat, zu überprüfen. In der DSFA ist auch anzugeben, wer die für die Einleitung der Überprüfung und Durchführung der Überprüfung **verantwortliche(n) Stelle(n)** (d. h. der für die Verarbeitung Verantwortliche, der Projektverantwortliche) und welches die **Kriterien** dafür sind, **eine außerordentliche Überprüfung** durchzuführen (d. h., Vorschläge, die erhebliche Veränderungen der Funktionalität des Fallbearbeitungssystems bedeuten, oder schwere Sicherheitsvorfälle oder sicherheitsrelevante Veränderungen).

3.4.2. Risiken

a) Präzisierung einiger der in der DSFA festgestellten Risiken erforderlich

Die EUStA sollte einige der in der DSFA festgestellten Risiken genauer präzisieren.

- **Risiko Nr. 10** betrifft Mängel bezüglich der **ordnungsgemäßen Unterrichtung betroffener Personen** über die Verarbeitung ihrer Daten. Die in der DSFA genannte Eindämmungsmaßnahme sieht vor, dass im Fallbearbeitungssystem angegeben wird, ob die Unterrichtung erfolgt ist oder, falls nicht, warum eine Beschränkung vorgenommen wurde. Die genannten Eindämmungsmaßnahmen berücksichtigen jedoch nicht Situationen, in denen „die Aussetzung oder Verzögerung der Unterrichtung der betroffenen Person" (wie in Artikel 4 Absatz 5 der Internen Datenschutzvorschriften der EUStA) nicht mehr gültig ist und die Unterrichtung der betroffenen Person dennoch noch nicht erfolgt ist.

Empfehlung 6: Analyse und Präzisierung weiterer Situationen, in denen die **Zurückstellung der Unterrichtung** betroffener Personen nicht mehr gilt; Gestaltung und Implementierung angemessener Eindämmungsmaßnahmen, um zu vermeiden, dass betroffene Personen in solchen Situationen nicht ordnungsgemäß unterrichtet werden.

- **Risiko 12** bezieht sich auf die Benachrichtigung der von einer „**Datenschutzverletzung**" betroffenen Personen.

  Artikel 75 Absatz 1 des Abkommens bestimmt: „Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt die EUStA die betroffene Person unverzüglich von der Verletzung." Artikel 8 der Internen Datenschutzvorschriften der EUStA enthält ferner die Bedingungen, die für die Benachrichtigung betroffener Personen über die Verletzung des Schutzes ihrer personenbezogenen Daten gelten. Der Klarheit halber sollte die EUStA auch hier die Terminologie anpassen, d. h. die Bezeichnung des Ereignisses sollte „Verletzung des Schutzes personenbezogener Daten" lauten, nicht „Sicherheitsverletzung".

Empfehlung 7: Präzisierung, dass

- es sich bei dem Ereignis um eine „Verletzung des Schutzes personenbezogener Daten" handelt;

- das Risiko die Benachrichtigung betroffener Personen über eine Verletzung des Schutzes ihrer personenbezogenen Daten betrifft, wenn die **Verletzung des Schutzes personenbezogener Daten** voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat.

- **Risiko 22** („**Aufnahme personenbezogener Daten ins Fallbearbeitungssystem ohne Kontext/Unterscheidungen z. B. hinsichtlich der Rolle der betroffenen Personen**") enthält folgende Angaben zum Risiko für die betroffene Person: „Betroffene **Personen**, die z. B. als Tatverdächtige, nicht als Zeugen, aufgeführt sind, oder Zeugen, die nicht als solche bezeichnet sind, wären einer stärker in ihre Rechte eingreifenden Verarbeitung ausgesetzt."

  Die Risikodefinition bezieht sich auf Situationen, in denen personenbezogene Daten ohne Unterscheidung hinsichtlich der Rolle der betroffenen Personen aufgenommen werden; in der Risikobeschreibung geht es jedoch darum, dass es vorkommen kann, dass die Angaben zu betroffenen Personen unrichtig sind. Die Eindämmungsmaßnahme wirkt auch nicht dem in der Risikodefinition genannten Problem entgegen, sondern greift nur in Situationen, in denen Daten/Metadaten fehlen; ein wichtiges Risiko ist aber gerade die Situation, dass die Angaben zu einer betroffenen Person unzutreffend sind.

Empfehlung 8: Präzisierung des Risikos/der Risiken bezüglich der Aufnahme personenbezogener Daten ins Fallbearbeitungssystem. Nach Ansicht des EDSB kann beides vorkommen: fehlende Metadaten wie auch falsche Angaben zu betroffenen Personen. Beide Fälle stellen gesonderte Risiken für die betroffenen Personen dar, und für jedes der Risiken sind geeignete Eindämmungsmaßnahmen vorzusehen.

- **Risiko 24** („**Bekanntermaßen unzutreffende, unvollständige oder rechtswidrig verarbeitete personenbezogene Daten werden Dritten übermittelt/zur Verfügung gestellt**“) enthält folgende Beschreibung des Risikos für die betroffene Person: „Wurden die Daten einer betroffenen Person nicht ordnungsgemäß verarbeitet, liegt die Verantwortung dafür, dies anderen Empfängern mitzuteilen, nicht bei der betroffenen Person, sondern bei der EUStA.“

  Die Risikobeschreibung passt nicht zu dem beschriebenen Ereignis. Das Risiko für die betroffenen Personen liegt darin, dass der Datenempfänger, falls die übermittelten Daten unzutreffend sind, möglicherweise gegen die betroffenen Personen ermittelt oder dass Fehlurteile gegen die betroffenen Personen ergehen.

Empfehlung 9: Präzisierung der Risikobeschreibung, so dass das Risiko für die betroffenen Personen ordnungsgemäß festgestellt und beschrieben wird und geeignete Maßnahmen dagegen getroffen werden.

- **Risiko 25** bezieht sich auf den Fall, dass dem EDSB „**der Zugang zu personenbezogenen Daten oder Verarbeitungsprotokollen, den er verlangt, nicht möglich ist**“. Die Risikobeschreibung lautet: „Die Aufsichtsfähigkeit des EDSB leidet, wenn ihm der Zugang, zu dem er berechtigt ist, nicht gewährt werden kann.“ Unter „Zugrunde liegender Datenschutzgrundsatz“ ist „Kontrolle durch den EDSB“ angegeben.

  Das in der DSFA genannte Risiko fokussiert auf die Aufsicht durch den EDSB, das Risiko für die betroffene Person ist jedoch nicht richtig beschrieben. So liegt z. B. eines der Risiken für betroffene Personen darin, dass sie möglicherweise nicht mehr in der Lage sind, ihre Rechte, so wie in Artikel 62 vorgesehen, über den EDSB auszuüben.

Empfehlung 10: Anpassung der Risikobeschreibung, um dem Risiko für die betroffenen Personen wie auch dem Inhalt der Spalte „Zugrunde liegender Datenschutzgrundsatz“ Rechnung zu tragen.

- **Risiko 28** betrifft den Fall, dass „**[d]em DSB der EUStA … der für die Wahrnehmung seiner Aufgaben erforderliche Zugang zu personenbezogenen Daten nicht möglich [ist]**“. Die Risikobeschreibung lautet: „Die Aufsichtsfähigkeit des DSB leidet, wenn der Zugang, zu dem er berechtigt ist, ihm nicht gewährt werden kann.“ Unter „Zugrunde liegender Datenschutzgrundsatz“ ist „Aufsicht“ angegeben.

  Das genannte Risiko fokussiert auf die Aufsicht durch den DSB, das Risiko für die betroffene Person ist jedoch nicht richtig beschrieben. So liegt z. B. eines der Risiken für betroffene Personen darin, dass diesen die unabhängige Überwachung der Einhaltung der Datenschutzvorschriften durch den DSB, so wie diese im Einzelnen in Artikel 79 der EUStA-Verordnung geregelt ist, möglicherweise nicht zugute kommt.

Empfehlung 11: Anpassung der Risikobeschreibung, um dem Risiko für die betroffenen Personen wie auch dem Inhalt der Spalte „Zugrunde liegender Datenschutzgrundsatz" Rechnung zu tragen.

- **Risiko 29** betrifft den Fall, dass die „**Beschränkung des Zugangs auf bestimmte Personen nicht möglich [ist], so dass jeder Zugang hat**". Die Risikobeschreibung lautet: „Werden personenbezogene Daten offengelegt, obwohl dies nicht erforderlich ist, ist das Restrisiko höher als bei Nichtoffenlegung."

Empfehlung 12: Präzisierung der Definition und Beschreibung dieses festgestellten Risikos, zum Beispiel, dass es gegeben ist, wenn Zugangslevel nicht auf Grundlage der Angewiesenheit auf die Informationen genau festgelegt werden. Außerdem ist die Risikobeschreibung durch Fokussierung auf das Risiko für die betroffenen Personen zu präzisieren.

- **Risiko 32** betrifft den Fall der „**Verarbeitung besonderer Kategorien personenbezogener Daten ohne entsprechende Begründung**". Die Beschreibung lautet: „Für besondere Kategorien personenbezogener Daten gelten bestimmte Beschränkungen. Werden diese nicht als solche bezeichnet, genießen sie möglicherweise weniger Schutz."

  Aus Risikodefinition und -beschreibung geht nicht klar hervor, ob sich das Risiko auf die rechtswidrige Verarbeitung besonderer Kategorien personenbezogener Daten (wie es in der Definition heißt) bezieht oder darauf, dass besondere Kategorien personenbezogener Daten „nicht als solche bezeichnet" sind (wie es in der Beschreibung heißt).

Empfehlung 13: Präzisierung der Definition und der Beschreibung des vorgenannten Risikos unter genauer Angabe und Hervorhebung der Risiken für die betroffenen Personen, zum Beispiel (wobei dies keine abschließende Aufzählung ist) mit der Erwähnung, dass für den Fall, dass besondere Kategorien personenbezogener Daten nicht ordnungsgemäß als solche bezeichnet werden, die betroffenen Personen möglicherweise einen geringeren Schutz genießen.

b) Einige in der DSFA übersehene Risiken

Der EDSB empfiehlt der EUStA, einige weitere Risiken in Betracht zu ziehen. Der EDSB hat diese zusätzlichen Risiken auf Grundlage der Verfahrensbeschreibung in der DSFA, der in der DSFA genannten Risiken und der gleichzeitig eingereichten Unterlagen festgestellt. Allerdings ist der EDSB nicht der Ansicht, dass, wenn diese Risiken zusätzlich in die DSFA aufgenommen würden, notwendigerweise eine erschöpfende Risikoanalyse gegeben wäre. Die EUStA wird gebeten, jetzt und auch später zu prüfen, ob diese Verarbeitung personenbezogener Daten andere Risiken für die betroffenen Personen mit sich bringt, die in künftigen Überprüfungen der DSFA zu berücksichtigen sind und denen entgegenzuwirken ist.

- **Zusätzliches Risiko 1: Nichteinhaltung der Verpflichtung zur Verarbeitung lediglich der für den Zuständigkeitsbereich der EUStA relevanten Daten (Rechtmäßigkeit)**

  Artikel 24 Absatz 7 der EUStA-Verordnung bestimmt: „Entscheidet die EUStA nach einer Prüfung, dass keine Gründe für die Einleitung eines Ermittlungsverfahrens … oder für die Ausübung ihres Evokationsrechts … vorliegen, so wird die Begründung im Fallbearbeitungssystem verzeichnet." Absatz 2 derselben Rechtsvorschrift lautet: „Die EUStA unterrichtet die Behörde, die die strafbare Handlung gemäß den Absätzen 1 und 2 gemeldet hat, sowie die Opfer der Straftat und, wenn dies im nationalen Recht so vorgesehen ist, andere Personen, die die strafbare Handlung gemeldet haben." Außerdem heißt es in Artikel 24 Absatz 8 der EUStA-Verordnung: „Erlangt die EUStA Kenntnis davon, dass möglicherweise eine nicht in ihre Zuständigkeit fallende Straftat begangen wurde, so unterrichtet sie unverzüglich die zuständigen nationalen Behörden und leitet alle sachdienlichen Beweise an sie weiter."

  Nach Artikel 49 Absatz 4 der EUStA-Verordnung „[darf] [d]ie EUStA … operative personenbezogene Daten vorübergehend verarbeiten, um festzustellen, ob diese Daten für ihre Aufgaben und … Zwecke relevant sind. … Nach Anhörung des Europäischen Datenschutzbeauftragten präzisiert das Kollegium die Bedingungen für die Verarbeitung derartiger operativer personenbezogener Daten, insbesondere in Bezug auf den Zugang zu den Daten und ihre Verwendung, sowie die Fristen für die Speicherung und Löschung der Daten."

  Artikel 37 Absatz 6 des Entwurfs der Geschäftsordnung der EUStA bestimmt, dass „[AUSLASSUNG]":

  In Abschnitt 5.*7.1. Einfügung und Registrierung operativer personenbezogener Daten*, *Abbildung 18 – Tabellarischer Überblick über Überprüfung und Registrierung* der DSFA heißt es: „Gespeicherte Informationen werden durch geeignetes Personal der EUStA bewertet, sofern die Informationen in den Aufgabenbereich fallen. Falls nicht, werden die Informationen zurückgewiesen, unter Umständen auch der Informationslieferant informiert, und/oder Daten an die zuständige Behörde, Einrichtung der Union übermittelt oder sonstige Maßnahmen ergriffen."

  Hinsichtlich des Verfahrens der Überprüfung, ob zugegangene personenbezogene Daten für die Aufgaben und Zwecke der EUStA relevant sind, sind in der DSFA folgende Risiken genannt: Risiko 1: „Rechtswidrige Verarbeitung personenbezogener Daten ohne Rechtsgrundlage für die Verarbeitung", woraus sich folgendes Risiko für die betroffene Person ergibt: „Die rechtswidrige Verarbeitung personenbezogener Daten bietet der betroffenen Person keinerlei Schutz oder Gewährleistung und beraubt sie ihrer Rechte auf den Schutz personenbezogener Daten." Als Eindämmungsmaßnahmen sind u. a. genannt: „detailliertes Verfahren für die Aufnahme personenbezogener Daten in das Fallbearbeitungssystem in Titel III der Geschäftsordnung (Artikel 37 ff)".

  Im Hinblick auf die in der DSFA, genauer gesagt in *Abbildung 18*, enthaltene Beschreibung und auf die Bestimmungen in Artikel 37 Absatz 6 des Entwurfs für die Geschäftsordnung der EUStA sowie um den Risiken für die betroffenen Personen angemessenen entgegenzuwirken und Risiken, die sich aus unklaren Verfahren ergeben können, zu vermeiden, sind weitere Präzisierungen zu den personenbezogenen Daten erforderlich, die der EUStA zugehen, aber nicht in ihren Zuständigkeitsbereich fallen.

Empfehlung 14: Angabe des Risikos, dass es vorkommen kann, dass durch unklare Verfahren für die Verarbeitung von Daten, die von der EUStA empfangen und vorübergehend verarbeitet werden, aber nicht in ihren Aufgabenbereich fallen, Risiken für betroffene Personen entstehen

(z. B., dass es keine klaren Arbeitsabläufe für solche Daten, insbesondere kein klares Verfahren für die Rückübermittlung der Daten an die zuständigen Behörden gibt, und dass es an spezifischen Voraussetzungen für diese Übermittlungen wie auch für die Datenlöschung fehlt).

- **Zusätzliches Risiko 2: Nichteinhaltung der Verpflichtung zur ordnungsgemäßen Reaktion auf Anträge betroffener Personen**
  Nach Artikel 59 der EUStA-Verordnung hat die betroffene Person das Recht, von der EUStA „eine Bestätigung darüber zu verlangen, ob operative personenbezogene Daten verarbeitet werden, die sie betreffen; ist dies der Fall, so hat sie ein Recht auf Auskunft über diese operativen personenbezogenen Daten" und auf bestimmte Informationen.

  In Abschnitt 5.*7.1. Einfügung und Registrierung operativer personenbezogener Daten*, *Abbildung 18 – Tabellarischer Überblick über Überprüfung und Registrierung* der DSFA heißt es: „[AUSLASSUNG]". Ähnlich heißt es in Abschnitt *6 Notwendigkeit und Verhältnismäßigkeit*: „… auf Daten, die im Fallbearbeitungssystem gespeichert, aber noch nicht registriert/überprüft sind, können Nutzer, die Suchen durchführen, nicht zugreifen".

  Wir nehmen zur Kenntnis, dass dieser Verfahrensschritt darauf ausgelegt ist, sicherzustellen, dass die EUStA nur die Daten verarbeitet, die für die Wahrnehmung ihrer Aufgaben relevant sind, so wie dies in den Bestimmungen in Artikel 49 Absatz 4 der EUStA-Verordnung vorgesehen ist. Wir nehmen auch zur Kenntnis, dass *Titel III – Operative Angelegenheiten/Kapitel 1 – Registrierung und Überprüfung von Informationen* des Entwurfs der Geschäftsordnung genauere Angaben zu den einschlägigen Bestimmungen für diese vorübergehende Verarbeitung personenbezogener Daten enthält.[6]

  Auch wenn die Verarbeitung nur vorübergehend erfolgt, handelt es sich dabei doch um eine Verarbeitung personenbezogener Daten, weshalb die Datenschutzvorschriften volle Anwendung finden. Wenn zum Beispiel eine betroffene Person anfragt, ob operative personenbezogene Daten über sie verarbeitet werden, und Auskunft dazu verlangt, sollte die EUStA in der Lage sein, zutreffend festzustellen, ob sie personenbezogene Daten des Antragstellers verarbeitet oder nicht.

Empfehlung 15: Aufnahme des Risikos, dass die Verpflichtung zur ordnungsgemäßen Reaktion auf Anträge betroffener Personen möglicherweise nicht erfüllt wird. Der EDSB **empfiehlt** der EUStA, zwischen registrierten personenbezogenen Daten (deren Überprüfung noch aussteht) und nicht registrierten personenbezogenen Daten zu unterscheiden und die jeweiligen Risiken für die zwei verschiedenen Fälle zu berücksichtigen. Des Weiteren sollte die EUStA in Erwägung ziehen, zwischen Registrierung und Überprüfung zu unterscheiden, da diese beiden Schritte mit unterschiedlichen Risiken verbunden sein könnten.

- **Zusätzliches Risiko 3: Nichteinhaltung des Grundsatzes der Speicherbegrenzung**

  Nach dem Grundsatz der „Speicherbegrenzung" (Artikel 47 Absatz 1 Buchstabe e) gilt, dass „[p]ersonenbezogene Daten … in einer Form gespeichert werden [müssen], die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist".

[6] Vgl. Schreiben des Europäischen Datenschutzbeauftragten an den Europäischen Generalstaatsanwalt vom 17. September 2020 sowie die beigefügten Anmerkungen [2020-0781 und 2020-0782].

Aus der DSFA und den beigefügten Unterlagen wird nicht deutlich, für welchen Zeitraum personenbezogene Daten „… die im Fallbearbeitungssystem gespeichert, aber noch nicht registriert/überprüft sind" aufbewahrt werden, bevor ein zuständiger Mitarbeiter der EUStA sie daraufhin überprüft, ob sie in den Aufgabenbereich fallen, und eine entsprechende Entscheidung erlässt. Nach Artikel 49 Absatz 4 der EUStA-Verordnung „[darf] [d]ie EUStA … operative personenbezogene Daten vorübergehend verarbeiten, um festzustellen, ob diese Daten für ihre Aufgaben und … Zwecke relevant sind". Des Weiteren ist dort vorgesehen, dass das Kollegium der EUStA nach Anhörung des EDSB „die Bedingungen für die Verarbeitung derartiger operativer personenbezogener Daten, insbesondere in Bezug auf den Zugang zu den Daten und ihre Verwendung, sowie die **Fristen für die Speicherung und Löschung der Daten** [präzisiert]".[7]

Empfehlung 16: Aufnahme des Risikos, dass Daten, die vorübergehend im Fallbearbeitungssystem gespeichert werden, um daraufhin registriert/überprüft zu werden, ob sie in den Zuständigkeitsbereich der EUStA fallen oder nicht, möglicherweise unter Verstoß gegen den Grundsatz der Speicherbegrenzung gespeichert werden. Als Eindämmungsmaßnahme empfiehlt der EDSB die Festlegung spezifischer Speicherungsfristen sowohl für die Zeit bis zur Registrierung der Daten als auch für Daten, die bereits registriert, aber noch nicht überprüft wurden.

- **Zusätzliches Risiko 4: Mangelhafte Entscheidungen wegen unzutreffender Daten über die tatverdächtige betroffene Person**

  Unter **Risiko 3** („**Möglichkeit der Verarbeitung unzutreffender Daten**") ist das Risiko für die betroffene Person in der DSFA wie folgt beschrieben: „Sind die personenbezogenen Daten unzutreffend, kann das dazu führen, dass eine andere betroffene Person ins Visier der Strafverfolgungsbehörden und etwaigen Ermittlungsmaßnahmen gerät."

Empfehlung 17: Vorsehen von Maßnahmen gegen ein anderes Risiko, das sich bei der Verarbeitung unzutreffender Daten ergeben kann, dass nämlich möglicherweise hinsichtlich der betroffenen Person, gegen die sich die Ermittlungen richten, falsche Entscheidungen getroffen werden.

- **Zusätzliches Risiko 5: Rechtswidrige Übermittlungen**

  Das Risiko, dass die EUStA operative personenbezogene Daten rechtswidrig – d. h. ohne dass Angemessenheit, geeignete Garantien oder Ausnahmen für die spezifische Situation gegeben sind – in einen Nicht-EU-Mitgliedstaat oder an eine internationale Organisation **übermittelt**, ist in der DSFA nicht aufgeführt und die DSFA sieht keine diesbezüglichen Maßnahmen vor.

Empfehlung 18: Aufnahme des Risikos und der Maßnahmen gegen die rechtswidrige Übermittlung operativer personenbezogener Daten an ein Drittland oder an eine internationale Organisation.

[7] Hervorhebungen nur hier.

- **Zusätzliches Risiko/zusätzliche Risiken 6: (Gemeinsame) Verantwortung für die Verarbeitung**

  Die DSFA berücksichtigt nicht die Risiken, die sich daraus ergeben, dass die Rollen, die mit der Verantwortlichkeit und/oder gemeinsamen Verantwortlichkeit der EUStA und der teilnehmenden Mitgliedstaaten verbunden sind, nicht eindeutig verstanden werden und nicht eindeutig definiert sind. Die Möglichkeit, dass sich Rechtsvorschriften (auf Unions- und nationaler Ebene) überschneiden, wird in der DSFA erwähnt: „da nationale Rechtsvorschriften weiterhin Anwendung finden und Ermittlungsverfahren und Strafverfolgung ihnen unterliegen".

Empfehlung 19: Aufnahme der Risiken, die sich daraus ergeben, dass die Rollen, die mit der **Verantwortlichkeit und/oder gemeinsamen Verantwortlichkeit** der EUStA und der teilnehmenden Mitgliedstaaten verbunden sind, nicht eindeutig verstanden werden und nicht eindeutig definiert sind.

- **Zusätzliches Risiko/zusätzliche Risiken 7: Einsatz von Auftragsverarbeitern/Unterauftragsverarbeitern**

  Die DSFA berücksichtigt nicht die Risiken, die mit dem Einsatz von Auftragsverarbeitern und ggf. Unterauftragsverarbeitern durch die EUStA verbunden sind. Da sich das mit der Verarbeitung personenbezogener Daten verbundene Risiko bei Einsatz von Auftragsverarbeitern und Unterauftragsverarbeitern erhöht, sollte dieser Aspekt in der DSFA berücksichtigt werden.

Empfehlung 20: Aufnahme der Risiken, die mit dem Einsatz von Auftragsverarbeitern und Unterauftragsverarbeitern durch die EUStA verbunden sind.

- **Zusätzliches Risiko/zusätzliche Risiken 8: Zugangsrechte**

  Das in der DSFA aufgeführte **Risiko 29** betrifft den Fall, dass die „**Beschränkung des Zugangs auf bestimmte Personen nicht möglich [ist], so dass jeder Zugang hat**". Einige der zusätzlichen Risiken in Bezug auf die Zugangsrechte zum Fallbearbeitungssystem sollten berücksichtigt werden, z. B.: versehentliche Zugangsgewährung an Personen, die keinen derartigen Zugang haben sollten; keine Sperrung des Zugangs für jemand, der nicht mehr an dem betreffenden Fall arbeitet; keine regelmäßige Überprüfung der zugewiesenen Rollen.

Empfehlung 21: Berücksichtigung der vorgenannten Risiken bezüglich der Zugangsrechte zum Fallbearbeitungssystem in der DSFA.

c) Unterschätzung der Auswirkungen von Risiken in bestimmten Fällen

Der EDSB empfiehlt der EUStA, die in der DSFA vorgenommene Beurteilung der Auswirkungen folgender Risiken zu überdenken.

- **Zu berücksichtigende Risikoauswirkung 1:**

  Unter **Risiko 3** („**Möglichkeit der Verarbeitung unzutreffender Daten**“) ist das Risiko für die betroffene Person in der DSFA wie folgt beschrieben: „Sind die personenbezogenen Daten unzutreffend, kann das dazu führen, dass eine andere betroffene Person ins Visier der Strafverfolgungsbehörden und etwaigen Ermittlungsmaßnahmen gerät.“ Die Auswirkung wird in der DSFA mit 3 eingestuft.

Empfehlung 22: Die Auswirkungen dieses Risikos (sowie des vom EDSB vorgeschlagenen zusätzlichen Risikos in Bezug auf die Verarbeitung unzutreffender Daten) sollten einer Neubewertung unterzogen werden, wobei auch zu prüfen ist, ob die Auswirkungen auf unzutreffender Datenbasis getroffener Entscheidungen für die betroffenen Personen nicht möglicherweise höher einzustufen sind. Für den Fall, dass die EUStA der Ansicht sein sollte, dass die Auswirkungen tatsächlich als 3 einzustufen sind, erwartet der EDSB eine Begründung.

- **Zu berücksichtigende Risikoauswirkung 2:**

  In **Risiko 4** („**Weitere Verarbeitung personenbezogener Daten über die vorgesehenen Fristen hinaus oder nachdem keine Notwendigkeit mehr besteht**“) enthält die DSFA die folgende Beschreibung des Risikos für die betroffene Person: „… Da die fehlende Notwendigkeit jedenfalls darauf hindeutet, dass es keinen Fokus auf die Daten gibt, gehen aus einer solchen weiteren Verarbeitung keine konkreten zusätzlichen Daten hervor.“ Die Auswirkung wird in der DSFA mit 1 eingestuft.

  Der EDSB ist der Ansicht, dass die Auswirkungen, die sich für die betroffenen Personen ergeben, wenn Speicherungsfristen nicht eingehalten werden, möglicherweise höher einzustufen sind. Des Weiteren ist es unbedingt erforderlich, im Fallbearbeitungssystem angemessene Aufbewahrungsfristen und -mechanismen zu definieren und zu implementieren, damit Daten, die nicht mehr benötigt werden, gekennzeichnet und gelöscht werden.

Empfehlung 23: Die Auswirkungen des Risikos der Überschreitung der Aufbewahrungsfrist sollten einer Neubewertung unterzogen werden, wobei auch zu prüfen ist, ob die Auswirkungen für die betroffenen Personen nicht möglicherweise höher einzustufen sind. Für den Fall, dass die EUStA der Ansicht sein sollte, dass die Auswirkungen tatsächlich als 1 einzustufen sind, erwartet der EDSB eine Begründung.

d) Unterschätzung der nach Eindämmungsmaßnahmen bestehenden Restwahrscheinlichkeit des Risikoeintritts (Risiko 14 – Ungewissheit hinsichtlich des einschlägigen Rechtsrahmens)

Laut DSFA ist die Restwahrscheinlichkeit von **Risiko 14 (Ungewissheit hinsichtlich des einschlägigen Rechtsrahmens für die Verarbeitung personenbezogener Daten)** nach Vornahme von Eindämmungsmaßnahmen als 1 einzustufen (ursprünglich war die Wahrscheinlichkeit vor Eindämmungsmaßnahmen als 4 eingestuft) Angesichts der Komplexität des einschlägigen Rechtsrahmens (Anwendbarkeit des unionsrechtlichen Rahmens und nationaler Rechtsvorschriften – Gesetze zur Umsetzung der Polizeirichtlinie sowie einschlägiges nationales Verfahrensrecht, wobei unter Umständen mehrere nationale

Rechtsvorschriften anwendbar sind, z. B. auch Strafprozessordnungen) fragt sich der EDSB, ob das Restrisiko möglicherweise unterschätzt wurde.

Empfehlung 24: Im Hinblick auf die Ungewissheit bezüglich des einschlägigen Rechtsrahmens sollte nochmals überprüft werden, ob die Restwahrscheinlichkeit des Risikoeintritts nach Eindämmungsmaßnahmen tatsächlich auf 1 reduziert werden kann.

e) Risikoeindämmung bewirkt keine Verringerung der Restwahrscheinlichkeit des Risikoeintritts (Risiko 25 – Kein Zugang des EDSB zu personenbezogenen Daten/Protokollen)

Laut der DSFA ist die Restwahrscheinlichkeit des Eintritts von **Risiko 25** („**Kein Zugang des EDSB zu personenbezogenen Daten/Protokollen**“) nach Eindämmungsmaßnahmen unverändert gleich hoch, nämlich mit 2 einzustufen.

Empfehlung 25: Neubewertung der Eindämmungsmaßnahmen, so dass die Restwahrscheinlichkeit des Risikoeintritts nach Maßnahmen zur Risikoeindämmung niedriger eingestuft wird.

3.5. Risikobewertung im Hinblick auf die Informationssicherheit

[AUSLASSUNG]

Empfehlung 26: [AUSLASSUNG]

****

4. EMPFEHLUNGEN

Erstens möchte der EDSB die insgesamt gute Qualität der DSFA hervorheben. In Anerkennung dieses positiven Aspekts hat der EDSB gleichwohl in dieser Stellungnahme einige Empfehlungen ausgesprochen, um die Einhaltung der Verordnung sicherzustellen. Der EDSB erwartet, dass die **vorgenannten Empfehlungen (siehe nachstehende Zusammenfassung)** innerhalb von **drei Monaten** nach dem Datum dieser Stellungnahme **implementiert** werden und die Implementierung **dokumentiert** wird.

1. Es ist sicherzustellen, dass die DSFA angepasst wird, um dem begrifflichen Unterschied zwischen „**Ereignissen**“ und „**Risiken**“ Rechnung zu tragen (Empfehlung 1).

2. Es ist sicherzustellen, dass der Abschnitt **Risikoeindämmung** zu jedem der Risiken Angaben zu spezifischen Maßnahmen zur Eindämmung des betreffenden Risikos enthält (Empfehlungen 2 und 3).
3. Die Überschrift der Spalte „**Zugrunde liegender Datenschutzgrundsatz**“ ist so anzupassen, dass sie sich auf Datenschutzvorschriften im Allgemeinen bezieht (Empfehlung 4).
4. Es ist sicherzustellen, dass in der DSFA angegeben ist, in welchen Abständen die DSFA nach der Inbetriebnahme des Fallbearbeitungssystems **überprüft** wird, welche **Stellen** für die Einleitung der Überprüfung und die Vornahme der Überarbeitung verantwortlich sind sowie nach welchen **Kriterien eine außerordentliche Überprüfung** stattfindet (Empfehlung 5).
5. Die in Abschnitt e der Stellungnahme genannten **Risiken** sind zu präzisieren (Empfehlungen 6-13).
6. Die in Abschnitt f der Stellungnahme genannten **zusätzlichen Risiken** sind zu bedenken (Empfehlungen 14-22).
7. Die **Auswirkungen** gewisser in Abschnitt g der Stellungnahme genannter Risiken sind neu zu bewerten (Empfehlungen 23 und 24). Was diese Empfehlungen angeht, erwartet der EDSB entweder eine Begründung der aktuellen Auswirkungseinstufung in der DSFA oder einen schriftlichen Nachweis für die Implementierung.
8. Es ist nochmals zu überprüfen, ob im Fall von Risiko 14 die **Restwahrscheinlichkeit** des Risikoeintritts nach Eindämmungsmaßnahmen tatsächlich auf 1 reduziert werden kann (Empfehlung 25).
9. Die Eindämmungsmaßnahmen für Risiko 25 sind einer Neubewertung zu unterziehen, so dass die **Restwahrscheinlichkeit** des Risikoeintritts nach Maßnahmen zur Risikoeindämmung niedriger eingestuft wird (Empfehlung 26).
10. Durchführung einer **Risikobewertung im Hinblick auf die Informationssicherheit** und Einsatz vorhandener technischer Lösungen im Fallbearbeitungssystem und deren **Sicherheitsmerkmale** (Empfehlung 27).

Brüssel, den 1. Oktober 2020

Wojciech Rafał WIEWIÓROWSKI