EUROPEAN DATA PROTECTION SUPERVISOR

Informelle Bemerkungen des EDSB zum Entwurf einer Datenschutz-Folgenabschätzung, der von […] zu einer Datenbank im Zusammenhang mit […] vorgelegt wurde (Fall 2021-0116)

Hintergrund

Das [EHI]

[...].

Rechtsrahmen

[...]

Es gibt daher eine klare Rechtsgrundlage für die Einrichtung einer […] Datenbank mit Informationen von [einschlägigen] Behörden in Bezug auf […] durch das [EHI].

Das Ersuchen

Am 29. Januar 2021 ersuchte […] den Europäischen Datenschutzbeauftragten (im Folgenden „EDSB“) um informelle Beratung zu einem Entwurf einer Datenschutz-Folgenabschätzung (im Folgenden „DSFA“) (im Folgenden „Ersuchen“).

Die DSFA bezieht sich auf die Pläne [des EHI], eine […] Datenbank für […] einzurichten. Das [EHI] *„begrüßt[e] den informellen Austausch mit dem Aufsichtsteam des EDSB“* in dieser Hinsicht.

Der Ansatz

Die DSFA wurde in erster Linie anhand der Grundsätze in Artikel 39 der Verordnung (EU) 2018/1725 (im Folgenden „EU-DSVO“)[1] und des Dokuments „Accountability on the ground Part II – Data Protection Impact Assessments & Prior Consultation“ (Rechenschaftspflicht in der Praxis Teil II – Datenschutz-Folgenabschätzungen und vorherige Konsultation) (im Folgenden „Instrumentarium zur Rechenschaftspflicht“)[2] des EDSB bewertet. Ferner wurden die Leitlinien zu DSFA und die Feststellung berücksichtigt, ob die Verarbeitung „voraussichtlich ein hohes Risiko [im Sinne der Verordnung (EU) 2016/679[3]] mit sich bringt“ , soweit sie analog anwendbar sind.

Die frühere Stellungnahme des EDSB zur vorherigen Konsultation durch die Europäischen Staatsanwaltschaft zu den in der DSFA zu ihrem Fallbearbeitungssystem ermittelten Risiken (im Folgenden „Stellungnahme des EDSB zur EUStA-DSFA“)[4] diente bei der Analyseals weiteres

[1] https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32018R1725
[2] https://edps.europa.eu/sites/edp/files/publication/19-07-17_accountability_on_the_ground_part_ii_en.pdf
[3] https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236
[4] https://edps.europa.eu/sites/edp/files/publication/20-10-01_prior_consultation_opinion_eppo_dpia_cms_2020-0568_en.pdf

Leitliniendokument.

Analyse der DSFA

Zunächst begrüßen wir, dass die DSFA der Vorlagenstruktur des DSFA-Berichts folgt, die im Instrumentarium zur Rechenschaftspflicht vorgesehen ist[5]. Wir werden die einzelnen Elemente der DSFA analysieren, um zu beurteilen, ob sie die von der EU-DSVO geforderten Informationen enthalten, die im Instrumentarium zur Rechenschaftspflicht weiter ausgeführt werden. Unsere wichtigsten Empfehlungen und Verbesserungsvorschläge sind in den nachstehenden Kommentaren unterstrichen.

1. Projektbezeichnung: Der Titel stellt in den Vordergrund, worum es bei der Verarbeitung geht. Dennoch wäre es leserfreundlicher, wenn das EHI auf eine etwas beschreibendere Formulierung zurückgreifen würde (z. B. „Die Einrichtung einer […] Datenbank… für […]… gemäß...“). Ferner schlagen wir vor, vor der Verwendung eines Akronyms im Text zu erläutern, wofür es steht (z. B. […]).

2. Validierung/Genehmigung: In der Liste ist die Genehmigungskette aufgeführt. Es ist jedoch nicht eindeutig, wer die DSFA letztendlich genehmigt. Es wird zwar der Schritt „*der für die Verarbeitung Verantwortliche genehmigt*“ erwähnt, aber der nächste Schritt scheint „*der für die Verarbeitung Verantwortliche erstattet dem ED Bericht*“ zu sein, wobei es sich bei Letzterem vermutlich um den Exekutivdirektor [des EHI] handelt. Die Genehmigung durch den ED, oder zumindest die Zurkenntnisnahme der von einem für die Verarbeitung Verantwortlichen genehmigten DSFA durch den ED, scheint zu fehlen. Zusammenfassend empfehlen wir, dass die Genehmigung der DSFA durch den Exekutivdirektor, d. h. die oberste Führungsebene, in der DSFA selbst unmissverständlich dargelegt wird.

3. Überprüfung: Der Text sieht Informationen über den aktuellen Stand der DSFA vor. Eine DSFA sollte ferner Informationen über den Überprüfungszyklus enthalten. Dem Instrumentarium zur Rechenschaftspflicht zufolge sollte sich die Länge des Überprüfungszyklus an den Risiken orientieren, die von der Verarbeitung ausgehen. Standardmäßig empfiehlt der EDSB einen Überprüfungszyklus von zwei Jahren, mit einer außerordentlichen Überprüfung im Falle von wesentlichen Veränderungen bei der Verarbeitung[6]. Es wird daher empfohlen, dass das [EHI] einen angemessenen Überprüfungszyklus in Betracht zieht und in der DSFA darauf verweist.

4. Zusammenfassung: Das [EHI] bietet einen guten Überblick über die Verarbeitung und die wichtigsten Risiken sowie die Maßnahmen zu deren Behebung, so wie sie derzeit in der DSFA stehen (siehe Punkt 9.f der DSFA). … Darüber hinaus ist zu erwähnen, dass das [EHI] die Notwendigkeit einer Vereinbarung über gemeinsam Verantwortliche mit [einschlägigen] Behörden gemäß den geltenden EDSB-Leitlinien in Betracht zieht[7]. Dies ist zu begrüßen. Wir gehen davon aus, dass das [EHI] zum gegebenen Zeitpunkt die entsprechenden Verpflichtungen und Zuständigkeiten in der besagten Vereinbarung in angemessenem Umfang festlegen wird.

5. Gründe für diese DSFA: Das [EHI] erläutert die Notwendigkeit der DSFA anhand von Argumenten, die im Einklang mit Artikel 39 der EU-DSVO stehen, sowie anhand der Elemente, die

[5] Siehe Anhang 3 des Instrumentariums zur Rechenschaftspflicht.
[6] Siehe Abschnitt 3.8 des Instrumentariums zur Rechenschaftspflicht.
[7] Leitlinien des EDSB zu den Begriffen „Verantwortlicher“, „Auftragsverarbeiter“ und „gemeinsam Verantwortliche“ nach der Verordnung (EU) 2018/1725: https://edps.europa.eu/sites/edp/files/publication/19-11-07_edps_guidelines_on_controller_processor_and_jc_reg_2018_1725_de.pdf.

in der Liste der Kriterien für die Bewertung, ob Verarbeitungen wahrscheinlich zu hohen Risiken führen, das enthalten ist im Dokument „Accountability on the ground Part I: Records, Registers and when to do Data Protection Impact Assessments“ (Rechenschaftspflicht in der Praxis Teil I: Aufzeichnungen, Register und wann Datenschutz-Folgenabschätzungen durchzuführen sind)[8]. Das [EHI] verweist ferner ausdrücklich auf den Beschluss des EDSB vom 16. Juli 2019 über die Listen der Datenschutz-Folgenabschätzungen, die gemäß Artikel 39 Absätze 4 und 5 der Verordnung (EU) 2018/1725 herausgegeben wurden[9]. Insgesamt verwendet das [EHI], wie in der Vorlage vorgeschlagen, eine Positivliste, die es darüber hinaus mit einer kurzen Erläuterung zu den Ergebnissen ergänzt. Dies ist zufriedenstellend.

6. **Hauptbeteiligte:** Im Instrumentarium zur Rechenschaftspflicht wird vorgeschlagen, an dieser Stelle einen Überblick darüber zu geben, *wer wann an welchem Teil beteiligt war*. Die vorgelegte Beschreibung ist mit dieser Anregung nicht unvereinbar. Allerdings ist sie zum jetzigen Zeitpunkt selbstverständlich eingeschränkt, da die DSFA noch ein Entwurf und nicht endgültig ist. Mit anderen Worten: Das [EHI] sollte sicherstellen, dass die entsprechenden Informationen im weiteren Verlauf vervollständigt werden.

7. **Beschreibung der Verarbeitung[10]:** Die DSFA folgt der Vorlage. Wir würden dem [EHI] dennoch empfehlen, hier eine ausführlichere Erläuterung hinsichtlich der Rechtsgrundlage aufzunehmen, und zwar durch eine genaue Beschreibung des Umfangs der anwendbaren Bestimmungen, damit sichergestellt wird, dass die DSFA ein eigenständiges Dokument ist, das verständlich ist, ohne dass der Leser auf andere Informationen zurückgreifen muss.

   (a) Die DSFA sieht ein **Datenfluss-Diagramm für das Verfahren (Ablaufplan)** vor, das die Interaktion zwischen den verschiedenen [einschlägigen] Interessenträgern mit der Datenbank erläutert;

   In der DSFA werden ferner (i) **die Datenquellen** erläutert. Hier wäre es jedoch hilfreich, wenn das [EHI] klar benennen würde (nicht nur mit Akronymen), wer die entsprechenden Behörden sind, und Fußnoten mit den einschlägigen Rechtsvorschriften einfügen würde, die im Text bereits erwähnt werden (insbesondere […]);

   Weiterhin wird in der DSFA (ii) aufgeführt, **welche Daten erhoben werden**. Hier empfehlen wir, eine kurze Erläuterung einiger Konzepte aufzunehmen, wenn auch nur in Fußnoten […].

   In der DSFA wird ferner erläutert, (iii) **was mit den Daten geschieht**, nämlich ihre Erhebung, Analyse, Weitergabe an [einschlägige] Behörden und Verwendung durch das [EHI] zum Zweck der [...]. Dies erscheint zufriedenstellend. Wir empfehlen jedoch, dass das [EHI] weiter erläutert, welche Analyse-Tools von Drittanbietern das [EHI] verwenden darf und welche Rollen und Zuständigkeiten diese Drittanbieter bei der tatsächlichen Verarbeitung haben.

   In der DSFA wird ferner erläutert, (iv) **wo und wie lange die Daten**

[8] Siehe die Vorlage für die Schwellenwertbewertung in Anhang 1 auf Seite 29: https://edps.europa.eu/sites/edp/files/publication/19-07-17_accountability_on_the_ground_part_i_en.pdf
[9] Siehe die Positivliste in Anhang 2 auf Seite 7: https://edps.europa.eu/sites/edp/files/publication/19-07-16_edps_dpia_list_en.pdf
[10] Artikel 39 Absatz 7 Buchstabe a EU-DSVO: *„Die Folgenabschätzung enthält zumindest […] eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung“.*

aufbewahrt werden. Die vorgeschlagene Aufbewahrungsfrist beträgt zehn Jahre. Das [EHI] erklärt, dass es im Einzelfall entscheiden kann, Daten vor Ablauf dieser Frist zu löschen. Es wird daher davon ausgegangen, dass es sich bei der Maßnahme, die standardmäßig nach Ablauf dieser 10-Jahres-Frist auf die aufbewahrten Daten angewendet wird, um die Löschung handelt. Es wäre jedoch sinnvoll, dies im Wortlaut der DSFA deutlich zu machen. Ferner wäre es angemessen, wenn das [EHI] die regelmäßige Bewertung der Notwendigkeit der in identifizierbarer Form aufbewahrten Daten besser erläutern würde.

Ebenso erkennt das [EHI] an, dass die in […] festgelegte standardmäßige Aufbewahrungsfrist fünf Jahre beträgt, jedoch unter bestimmten Umständen um weitere fünf Jahre verlängert werden kann […]. Diesbezüglich argumentiert das [EHI], dass die Aufbewahrungsfristen in den Mitgliedstaaten unterschiedlich sind, und betont, dass das Thema der Aufbewahrung in einem ähnlichen Fall bereits vom EDSB in einer Stellungnahme […] zu einer früheren Überprüfung aufgegriffen wurde. […] ferner ist das [EHI] bereit, die Aufbewahrungsfrist neu zu bewerten und anzupassen, wenn sie sich als unverhältnismäßig oder unzureichend erweist. Hier lohnt es sich daher, dem [EHI] in Übereinstimmung mit der Stellungnahme des EDSB […] zu empfehlen, dass, wenn das [EHI] die ersten zehn Jahre Praxis durchlaufen hat […], eine Bewertung der Notwendigkeit des 10-Jahres-Zeitraums vorgenommen werden sollte. Auf der Grundlage einer solchen Bewertung sollte das [EHI] in der Lage sein nachzuweisen, ob eine derartige längere Aufbewahrungsfrist tatsächlich erforderlich ist;

Schließlich erläutert das [EHI] (v), **wohin und auf welcher Grundlage es die Daten übermittelt**: in der DSFA werden die [entsprechenden] Behörden aufgeführt, an die es Daten übermitteln darf. Obwohl dies grundsätzlich zufriedenstellend zu sein scheint, könnte argumentiert werden, dass weitere Einzelheiten angegeben werden sollten, nämlich nach Möglichkeit die genauen Verweise auf die erwähnten Protokolle und Absichtserklärungen.

(b) Detaillierte Beschreibung der Verarbeitungszwecke: Im Instrumentarium zur Rechenschaftspflicht wird vorgeschlagen, dass das [EHI] den Prozess Schritt für Schritt erläutern und dabei, wo nötig, zwischen den Zwecken unterscheidet. Das [EHI] scheint Informationen bereitzustellen, die angesichts der Tatsache, dass sich das Projekt noch in einem sehr frühen Stadium befindet, wahrscheinlich zufriedenstellend sind.

(c) Beschreibung der Zusammenhänge mit anderen Vorgängen: Die Erläuterung erscheint in dieser Hinsicht zufriedenstellend zu sein. Es erscheint jedoch sinnvoll zu klären, wie Daten aus Datenbanken oder Plattformen, die bereits vom [EHI] verwaltet werden, eingepflegt werden. Zunächst sollte zur Stärkung des Grundsatzes der Rechenschaftspflicht eine umfassendere rechtliche Analyse zur Zweckkompatibilität angegangen werden. Anschließend ist eine technische und organisatorische Erläuterung erforderlich, um eventuelle Risiken besser zu verstehen.

(d) Beschreibung der unterstützenden Infrastruktur: Diese wurde bisher nicht definiert. Eine genaue Beschreibung der Infrastruktur mit besonderem Augenmerk auf die Funktion der gemeinsamen Datennutzung ist von größter Bedeutung für die

Bewertung der Einhaltung der gesetzlichen Anforderungen und möglicher Risiken, die sich aus der Anwendung ergeben. Darüber hinaus sollte eine gründliche Risikobewertung der Informationssicherheit durchgeführt werden, um die Eignung der technischen und organisatorischen Maßnahmen zur Sicherheit der personenbezogenen Daten und der IT-Systeme, die deren Verarbeitung unterstützen, gemäß Artikel 4 Absatz 1 Buchstabe f und Artikel 33 der EU-DSVO sowie dem Instrumentarium zur Rechenschaftspflicht nachzuweisen.

8. Notwendigkeit und Verhältnismäßigkeit[11]: Dieser Punkt ist falsch nummeriert: er sollte einen separaten Punkt (8) darstellen und nicht eine zusätzliche Unterkategorie (e) der in Punkt (7) des Entwurfs zur DSFA enthaltenen Beschreibungen. Das [EHI] scheint ausreichend zu erläutern, (a) warum die personenbezogenen Daten zur Erfüllung des ihm übertragenen Mandats erforderlich sind. Hinsichtlich (b) der Verhältnismäßigkeit, d. h. der Frage, ob die erforderlichen Daten ferner innerhalb der Grenzen des zur Erfüllung der Aufgaben Angemessenen liegen, verweist das [EHI] im Wesentlichen auf die Sachdienlichkeit und die Richtigkeit der verwendeten Daten sowie auf die vorhandenen Garantien, die eine ordnungsgemäße Verarbeitung dieser Daten gewährleisten. In Übereinstimmung mit Artikel 39 Absatz 6 Buchstabe b der EU-DSVO verlangt das Instrumentarium zur Rechenschaftspflicht eine Gegenüberstellung der Vorteile der Verarbeitung und der Risiken für die Grundrechte, die von der Verarbeitung ausgehen. Wir würden empfehlen, dass das [EHI] eine eindeutige Stellungnahme dazu abgibt, warum die Verarbeitung in der geplanten Form verhältnismäßig ist, um sicherzustellen, dass das [EHI] sein Mandat erfüllt.

9. Analyse der Risiken und Einrichtung von Kontrollen für identifizierte Risiken[12]: Dieser Punkt ist falsch nummeriert: er sollte einen separaten Punkt (9) darstellen und nicht eine zusätzliche Unterkategorie (f) der in Punkt (7) des Entwurfs zur DSFA enthaltenen Beschreibungen.

Im Instrumentarium zur Rechenschaftspflicht wird vorgeschlagen, dass der Schwerpunkt in erster Linie auf den Risiken für die Rechte und Freiheiten der betroffenen Personen und dann auf den Compliance-Risiken für das Institut liegen sollte, und zwar nicht nur für den Fall, dass etwas nicht funktioniert, sondern auch für den Fall, dass alle Prozesse wie geplant funktionieren.

Der Entwurf zur DSFA scheint genau das vorzusehen und die Analyse scheint auf einem guten Stand zu sein, erfordert jedoch weitere Fortschritte in Bezug auf spezifische Merkmale, die noch definiert werden müssen. Insbesondere die Ausgestaltung und die Effektivität der Kontrollen und Abhilfemaßnahmen in Bezug auf die Risiken Nr. 12 und 13 sollten besser erläutert werden, um den beabsichtigten verbleibende Schweregrad und die beabsichtigte verbleibende Wahrscheinlichkeit zu erreichen.

10. Anmerkungen der betroffenen Personen (falls zutreffend): In Anbetracht des Umfangs der Verarbeitung, auf die sich die DSFA bezieht, erscheint es angemessen, dass keine Konsultation der betroffenen Personen vorgesehen ist.

11. Bemerkungen des DSB: Die Informationen sind möglicherweise im Laufe der Arbeiten

[11] Artikel 39 Absatz 7 Buchstabe b EU-DSVO: *„Die Folgenabschätzung enthält zumindest […] eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf die Zwecke“.*

[12] Artikel 39 Absatz 7 Buchstabe c EU-DSVO: *„Die Folgenabschätzung enthält zumindest […] eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen...“* und Artikel 39 Absatz 7 Buchstabe b EU-DSVO: *„Die Folgenabschätzung enthält zumindest […] die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.“*

an der DSFA zu aktualisieren.

Zusammenfassung der Empfehlungen und Verbesserungsvorschläge des EDSB

Empfehlungen:

- Eindeutige Erläuterung, wer die DSFA genehmigt;
- Aufnahme eines angemessenen Überprüfungszyklus der DSFA;
- Bessere Beschreibung der anwendbaren gesetzlichen Bestimmungen, insbesondere durch exakte Verweise;
- Gewährleistung, dass die zukünftigen Vereinbarungen über gemeinsam Verantwortliche die erforderlichen Informationen zum Verständnis der Pflichten und Zuständigkeiten der gemeinsam Verantwortlichen enthalten;
- Aktualisierung der Informationen über die Hauptbeteiligten im Zuge der Weiterentwicklung des Projekts;
- Eindeutige Angabe der Quellen der Daten und Verweise auf einschlägige gesetzliche Bestimmungen;
- Erläuterung der Konzepte, die in dem Teil über die erhobenen Daten verwendet werden, wie z. B. […];
- Erläuterung, welche Analyseinstrumente von Drittanbietern verwendet werden können, und Klärung der Rollen und Zuständigkeiten der genannten Drittanbieter;
- Eindeutige Erläuterung, was mit den Daten nach Ablauf der Aufbewahrungsfrist geschieht;
- Bessere Erläuterung, wie die regelmäßige Bewertung der Notwendigkeit der in identifizierbarer Form aufbewahrten Daten durchgeführt wird;
- Wann immer es dem [EHI] möglich ist, eine Bewertung der Notwendigkeit der 10-jährigen Aufbewahrungsfrist vorzunehmen, Nachweis, ob eine so lange Aufbewahrungsfrist tatsächlich notwendig ist;
- Wenn möglich, Aufnahme von Verweisen auf genaue Protokolle und Absichtserklärungen zu Datenübertragungen;
- Klarstellung, wie Daten aus Datenbanken oder Plattformen, die bereits vom [EHI] verwaltet werden, eingepflegt werden;
- Beschreibung der Infrastruktur mit besonderem Schwerpunkt auf der Funktion zum Datenaustausch;
- Verweis auf die durchgeführte gründliche Bewertung der Informationssicherheitsrisiken;
- Aufnahme eines gesonderten Punktes (8) für die Notwendigkeit und Verhältnismäßigkeit; Aufnahme einer eindeutigen Erklärung, warum das [EHI] die Daten für verhältnismäßig hält; und
- Aufnahme eines gesonderten Punktes (9) zur Analyse der Risiken und zur Einrichtung von Kontrollen für die identifizierten Risiken;
Bessere Erläuterung des Aufbaus und der Wirksamkeit der Kontrollen und Abhilfemaßnahmen in Bezug auf die Risiken Nr. 12 und 13.

Sonstige Verbesserungsvorschläge

- Erwägung eines aussagekräftigeren Titels und Erläuterung der Bedeutung der Akronyme; und
- Erwägung der Veröffentlichung der DSFA oder zumindest einer Zusammenfassung davon auf der Website des EHI, sobald diese abgeschlossen ist.

26. Februar 2021