Stellungnahme des EDSA nach Artikel 64 DSGVO

Stellungnahme 17/2018

zu der von den zuständigen Aufsichtsbehörden Polens entworfenen Liste

der

Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist (Artikel 35 Absatz 4 DSGVO)

angenommen am 25. September 2018

Inhalt

Der Europäische Datenschutzausschuss –

gestützt auf Artikel 63, Artikel 64 Absatz 1 Buchstabe a, Absätze 3 bis 8 und Artikel 35 Absätze 1, 3, 4 und 6 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung, im Folgenden „DSGVO“),

gestützt auf das Abkommen über den Europäischen Wirtschaftsraum, insbesondere auf Anhang XI und Protokoll 37 in der durch den Beschluss Nr. 154/2018 des Gemeinsamen EWR-Ausschusses vom 6. Juli 2018 geänderten Fassung,

gestützt auf die Artikel 10 und 22 seiner Geschäftsordnung vom 25. Mai 2018,

in Erwägung nachstehender Gründe:

(1) Die Hauptaufgabe des Ausschusses besteht darin, eine kohärente Anwendung der DSGVO im gesamten Europäischen Wirtschaftsraum sicherzustellen. Gemäß Artikel 64 Absatz 1 DSGVO hat der Ausschuss eine Stellungnahme abzugeben, wenn eine Aufsichtsbehörde beabsichtigt, in Übereinstimmung mit Artikel 35 Absatz 4 eine Liste der Verarbeitungsvorgänge anzunehmen, für die eine Datenschutz-Folgenabschätzung durchzuführen ist. Durch diese Stellungnahme soll daher ein einheitlicher Ansatz für Verarbeitungsvorgänge geschaffen werden, die grenzüberschreitenden Charakter besitzen oder Auswirkungen auf den freien Verkehr personenbezogener Daten natürlicher Personen in der Europäischen Union haben können. Die DSGVO sieht zwar nicht vor, dass nur genau eine solche Liste zu erstellen ist, soll aber für Kohärenz sorgen. Um dies zu erreichen, empfiehlt der Ausschuss den Aufsichtsbehörden in seinen Stellungnahmen jeweils, bestimmte Verarbeitungsvorgänge in ihre Listen aufzunehmen, bestimmte Kriterien, die nach Auffassung des Ausschusses nicht zwangsläufig hohe Risiken für die betroffenen Personen mit sich bringen, von ihren Listen zu streichen oder bestimmte Kriterien einheitlich anzuwenden.

(2) Gemäß Artikel 35 Absätze 4 und 6 DSGVO haben die zuständigen Aufsichtsbehörden Listen der Verarbeitungsvorgänge zu erstellen, für die eine Datenschutz-Folgenabschätzung (im Folgenden „DSFA“) durchzuführen ist. Dabei sind sie gehalten, das in der DSGVO vorgesehene Kohärenzverfahren anzuwenden, wenn solche Listen Verarbeitungstätigkeiten umfassen, die mit dem Angebot von Waren oder Dienstleistungen für betroffene Personen oder der Beobachtung des Verhaltens dieser Personen in mehreren Mitgliedstaaten im Zusammenhang stehen oder die den freien Verkehr personenbezogener Daten innerhalb der Union erheblich beeinträchtigen könnten.

(3) Dass die von den zuständigen Aufsichtsbehörden zu erstellenden Listen dem Kohärenzverfahren unterliegen, bedeutet jedoch nicht, dass die Listen identisch sein

müssen. Die zuständigen Aufsichtsbehörden verfügen nämlich über einen Ermessensspielraum bezüglich des nationalen oder regionalen Kontextes und haben ihren lokalen Rechtsvorschriften Rechnung zu tragen. Diese Bewertung bzw. Stellungnahme des EDSA stellt nicht darauf ab, dass eine einheitliche EU-weite Liste aufgestellt wird. Sie soll vielmehr große Inkohärenzen vermeiden, die einem gleichwertigen Schutz der betroffenen Personen abträglich sind.

(4) Gemäß Artikel 35 Absatz 1 DSGVO ist eine DSFA für den Verantwortlichen nur dann obligatorisch, wenn die beabsichtigte Verarbeitung „voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge“ hat. In Artikel 35 Absatz 3 DSGVO sind exemplarisch mehrere Fälle genannt, in denen ein solches hohes Risiko bestehen kann. Diese Aufzählung ist nicht erschöpfend. Die Datenschutzgruppe nach Artikel 29 (WP29) hat in ihren Leitlinien zur Datenschutz-Folgenabschätzung (WP248)[1], die vom EDSA gebilligt worden sind[2], die Kriterien präzisiert, anhand der sich ermitteln lässt, ob für die geplanten Verarbeitungsvorgänge eine DSFA erforderlich ist. In diesen Leitlinien heißt es, dass wenn ein Verarbeitungsvorgang zwei dieser Kriterien erfüllt, der für die Datenverarbeitung Verantwortliche („der Verantwortliche“) in den meisten Fällen zu dem Schluss kommen muss, dass eine DSFA obligatorisch ist, es in einigen Fällen jedoch vorkommen kann, dass ein für die Datenverarbeitung Verantwortlicher von der Notwendigkeit einer DSFA ausgehen muss, obwohl der fragliche Verarbeitungsvorgang nur eines dieser Kriterien erfüllt.

(5) Die von den zuständigen Aufsichtsbehörden erstellten Listen dienen ebenfalls dem Ziel, Verarbeitungsvorgänge zu ermitteln, die wahrscheinlich ein hohes Risiko mit sich bringen und bei denen daher gegebenenfalls eine DSFA erforderlich ist. Die in den Leitlinien der Datenschutzgruppe nach Artikel 29 dargelegten Kriterien sollten daher bei der Prüfung der Frage herangezogen werden, ob die von den zuständigen Aufsichtsbehörden erstellten Listen einer kohärenten Anwendung der DSGVO nicht im Wege stehen.

(6) Zweiundzwanzig zuständige Aufsichtsbehörden haben dem EDSA ihre Listenentwürfe übermittelt. Die Gesamtbewertung dieser Listenentwürfe dient dem Ziel einer kohärenten Anwendung der DSGVO, wenngleich sich dadurch die Komplexität des Themas erhöht.

(7) Gemäß Artikel 64 Absatz 3 DSGVO in Verbindung mit Artikel 10 Absatz 2 der Satzung des EDSA hat die Annahme der Stellungnahme des EDSA binnen acht Wochen ab dem ersten Werktag, nachdem der Vorsitz und die zuständige Aufsichtsbehörde beschlossen haben, dass die Akte abgeschlossen ist, zu erfolgen. Diese Frist kann unter Berücksichtigung der Komplexität der Angelegenheit auf Beschluss des Vorsitzes um sechs Wochen verlängert werden –

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

[1] 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“ (WP 248 Rev. 01).
[2] EDSA, Billigung 1/2018.

1. Zusammenfassung des Sachverhalts

Das Amt für den Schutz personenbezogener Daten (im Folgenden „die polnische Aufsichtsbehörde“) hat seinen Listenentwurf dem EDSA übermittelt. Der Beschluss über den Abschluss der Akte erging am 20. Juni 2018. Die Frist für die Annahme der Stellungnahme ist unter Berücksichtigung der Komplexität der Angelegenheit und angesichts der Tatsache, dass gleichzeitig 22 zuständige Aufsichtsbehörden ihre Listenentwürfe eingereicht haben und daher eine Gesamtbewertung erforderlich geworden ist, bis zum 25. September verlängert worden.

2. Bewertung

2.1 Allgemeine Anmerkungen des EDSA zu der eingereichten Liste

Alle dem EDSA vorgelegten Listen sind als nähere Spezifizierung von Artikel 35 Absatz 1 ausgelegt worden, der in jedem Fall maßgeblich bleiben wird. Folglich kann keine Liste erschöpfend sein. Da darauf in der von der polnischen Aufsichtsbehörde vorgelegten Liste nicht ausdrücklich hingewiesen wird, sollte dieser Hinweis in das Dokument mit der Liste eingefügt werden.

Der EDSA vertritt in Übereinstimmung mit Artikel 35 Absatz 10 DSGVO die Auffassung, dass in Fällen, in denen bereits im Rahmen der allgemeinen Folgenabschätzung im Zusammenhang mit dem Erlass der Rechtsgrundlage eine DSFA durchgeführt wurde, die Absätze 1 bis 7 des Artikels 35 nur gelten, wenn nach dem Ermessen des Mitgliedstaats eine DSFA erforderlich ist.

Ferner sollte die polnische Aufsichtsbehörde in Fällen, in denen der EDSA eine DSFA für eine bestimmte Verarbeitungskategorie empfiehlt, das nationale Recht aber bereits eine gleichwertige Maßnahme vorsieht, einen Verweis auf diese Maßnahme hinzufügen.

In dieser Stellungnahme werden alle von der polnischen Aufsichtsbehörde angesprochenen Punkte, die nach Auffassung des EDSA nicht in den Anwendungsbereich von Artikel 35 Absatz 6 DSGVO fallen, unberücksichtigt gelassen. Damit sind Verarbeitungstätigkeiten gemeint, die nicht „mit dem Angebot von Waren oder Dienstleistungen für betroffene Personen oder der Beobachtung des Verhaltens dieser Personen in mehreren Mitgliedstaaten im Zusammenhang stehen“ oder bei denen es unwahrscheinlich ist, dass sie „den freien Verkehr personenbezogener Daten innerhalb der Union erheblich beeinträchtigen“ können. Dies gilt besonders für in den nationalen Rechtsvorschriften vorgesehene Verarbeitungsvorgänge und insbesondere für den Fall, dass diese Rechtsvorschriften eine DSFA vorsehen. Darüber hinaus hat der EDSA alle etwaig aufgeführten Verarbeitungsvorgänge, die zu Strafverfolgungszwecken erfolgen, unberücksichtigt gelassen, da diese nach seiner Auffassung nicht in den Anwendungsbereich der DSGVO fallen.

Der EDSA hat festgestellt, dass mehrere Aufsichtsbehörden auf ihren Listen auch Verarbeitungsvorgänge aufgeführt haben, die zwangsläufig nur auf lokaler Ebene durchgeführt werden können. Da sich Artikel 35 Absatz 6 DSGVO aber nur auf Verarbeitungsvorgänge bezieht, die grenzüberschreitenden Charakter besitzen oder Auswirkungen auf den freien Verkehr personenbezogener Daten natürlicher Personen in der Europäischen Union haben können, geht der EDSA auf diese lokalen Verarbeitungsvorgänge nicht ein.

In dieser Stellungnahme wird ein kohärenter Kern von Verarbeitungsvorgängen definiert, die auf allen von den Aufsichtsbehörden eingereichten Listen aufgeführt sind.

Für die begrenzte Zahl von Verarbeitungsvorgängen, für die der EDSA eine einheitliche Definition festlegt, sollten alle Aufsichtsbehörden eine DSFA vorschreiben. Der EDSA wird den Aufsichtsbehörden empfehlen, ihre Listen entsprechend zu ändern, damit Kohärenz sichergestellt wird.

Wird in dieser Stellungnahme nicht auf Datenschutzfolgeabschätzungen eingegangen, die auf der eingereichten Liste aufgeführt sind, bedeutet dies, dass der EDSA der polnischen Aufsichtsbehörde diesbezüglich keine weiteren Maßnahmen empfiehlt.

Zuletzt möchte der EDSA daran erinnern, dass sowohl für alle für die Datenverarbeitung Verantwortlichen als auch für die Auftragsverarbeiter Transparenz oberstes Gebot sein muss. Diese Transparenz ließe sich verbessern, wenn bei jedem auf der Liste aufgeführten Verarbeitungsvorgang zur näheren Präzisierung explizit auf die betreffenden Kriterien der Leitlinien verwiesen würde. Der EDSA ist daher der Auffassung, dass der Liste eine Erläuterung hinzugefügt werden könnte, welche Kriterien von der polnischen Aufsichtsbehörde bei der Aufstellung der Liste berücksichtigt wurden.

2.2 Anwendung des Kohärenzverfahrens auf den Listenentwurf

Der von der polnischen Aufsichtsbehörde eingereichte Listenentwurf bezieht sich, da die auf ihm aufgeführten Verarbeitungsvorgänge nicht auf betroffene Personen in Polen begrenzt sind, auf Verarbeitungstätigkeiten, die mit dem Angebot von Waren oder Dienstleistungen für betroffene Personen oder der Beobachtung des Verhaltens dieser Personen in mehreren Mitgliedstaaten im Zusammenhang stehen oder die den freien Verkehr personenbezogener Daten innerhalb der Union erheblich beeinträchtigen könnten.

2.3 Analyse des Listenentwurfs

Unter Berücksichtigung der Tatsache, dass

a. Artikel 35 Absatz 1 DSGVO eine DSFA in allen Fällen vorschreibt, in denen die beabsichtigte Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, und
b. Artikel 35 Absatz 3 DSVGO eine nicht erschöpfende Liste von Verarbeitungsvorgängen vorsieht, die eine DSFA erfordern,

gelangt der EDSA zu folgender Stellungnahme:

Indikativer Charakter der Liste

Da in der von der polnischen Aufsichtsbehörde vorgelegten Liste nicht ausdrücklich darauf hingewiesen wird, dass die Liste nicht erschöpfend ist, sollte dieser Hinweis in das Dokument mit der Liste eingefügt werden.

Verweis auf die Leitlinien

Nach dem Dafürhalten des EDSA ist die Analyse, die die Datenschutzgruppe nach Artikel 29 in ihren Leitlinien vorgenommen hat, eine zentrale Voraussetzung für die Sicherstellung von Kohärenz in der gesamten Union. Der EDSA empfiehlt daher den verschiedenen Aufsichtsbehörden, in das Dokument mit der Liste eine Erklärung einzufügen, durch die klargestellt wird, dass die Liste auf den Leitlinien basiert und diese ergänzt und näher spezifiziert.

Da das von der polnischen Aufsichtsbehörde vorgelegte Dokument keine solche Erklärung enthält, empfiehlt der EDSA der polnischen Aufsichtsbehörde, das Dokument entsprechend zu ändern.

Biometrische Daten

Die Liste, die dem EDSA von der polnischen Aufsichtsbehörde zur Stellungnahme vorgelegt wurde, sieht bisher für Verarbeitungsvorgänge, bei denen biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person verarbeitet werden, keine DSFA vor. Der EDSA empfiehlt der polnischen Aufsichtsbehörde daher, die Liste entsprechend zu ändern und sie unbeschadet von Artikel 35 Absatz 3 DSGVO ausdrücklich um die Verarbeitung biometrischer Daten zur eindeutigen Identifizierung einer natürlichen Person in Verbindung mit mindestens einem weiteren auf der Liste aufgeführten Kriterium zu erweitern.

Genetische Daten

Die Liste, die dem EDSA von der polnischen Aufsichtsbehörde zur Stellungnahme vorgelegt wurde, sieht bisher für Verarbeitungsvorgänge, bei denen genetische Daten verarbeitet werden, keine DSFA vor. Nach dem Dafürhalten des EDSA bringt die Verarbeitung genetischer Daten als solche nicht zwangsläufig ein hohes Risiko mit sich. Wenn sie jedoch in Verbindung mit mindestens einem der anderen Kriterien erfolgt, ist eine DSFA erforderlich. Der EDSA empfiehlt der polnischen Aufsichtsbehörde daher, die Liste entsprechend zu ändern und sie unbeschadet von Artikel 35 Absatz 3 DSGVO ausdrücklich um die Verarbeitung genetischer Daten in Verbindung mit mindestens einem weiteren auf der Liste aufgeführten Kriterium zu erweitern.

Standortdaten

Der EDSA ist der Auffassung, dass die Schaffung von Kohärenz eines der Grundprinzipien der DSGVO ist. Der EDSA stellt fest, dass auf den meisten eingereichten Listen ausdrücklich die Verarbeitung von Standortdaten aufgeführt wird. Da dies bei der Liste, die dem EDSA von der polnischen Aufsichtsbehörde zur Stellungnahme vorgelegt wurde, nicht der Fall ist,

empfiehlt der EDSA der polnischen Aufsichtsbehörde, die in Verbindung mit einem weiteren Kriterium erfolgende Verarbeitung von Standortdaten in ihre Liste aufzunehmen.

Überwachung von Beschäftigten

Nach Auffassung des EDSA können Verarbeitungsvorgänge, die zum Zweck der Überwachung von Beschäftigten erfolgen, aufgrund ihres besonderen Charakters und des Umstands, dass sie das in den Leitlinien angesprochene Kriterium schutzbedürftiger betroffener Personen und ihrer systematischen Überwachung erfüllen, eine DSFA erforderlich machen. Da in der Liste, die dem EDSA von der polnischen Aufsichtsbehörde zur Stellungnahme vorgelegt wurde, bereits vorgesehen ist, dass für derartige Verarbeitungsvorgänge eine DSFA erforderlich ist, möchte der EDSA diesbezüglich lediglich die Empfehlung hinzufügen, dass bezüglich der zwei Kriterien explizit auf die Leitlinien der Datenschutzgruppe nach Artikel 29 (WP248) verwiesen werden sollte. Zudem ist der EDSA der Auffassung, dass die Stellungnahme, die die Datenschutzgruppe nach Artikel 29 zum Thema Datenverarbeitung am Arbeitsplatz (WP249) abgegeben hat, für die Definition dessen, was unter einer systematischen Verarbeitung von Mitarbeiterdaten zu verstehen ist, weiterhin ihre Gültigkeit behält.

Abweichungen von den Leitlinien

Der EDSA hat festgestellt, dass die polnische Aufsichtsbehörde in den Punkten 2, 4, 5, 6, 8 und 9 ihrer Liste die Kriterien der Leitlinien der Datenschutzgruppe nach Artikel 29 aufgreift. In diesen Leitlinien heißt es jedoch, dass wenn ein Verarbeitungsvorgang zwei dieser Kriterien erfüllt, der für die Datenverarbeitung Verantwortliche in den meisten Fällen zu dem Schluss kommen muss, dass eine DSFA obligatorisch ist. Insofern ist der EDSA der Auffassung, dass die von der polnischen Aufsichtsbehörde vorgelegte Liste nicht im Einklang mit den Leitlinien steht. Daher empfiehlt der EDSA der polnischen Aufsichtsbehörde, ihre Liste in Einklang mit den Leitlinien zu bringen, indem hinzugefügt wird, dass bei den vorgenannten Punkten eine DSFA in den meisten Fällen nur erforderlich ist, wenn bei der betreffenden Verarbeitung zwei Kriterien erfüllt sind, und dass unabhängig davon, welche Maßnahmen der Verantwortliche zu ergreifen gedenkt, die Wahrscheinlichkeit, dass eine Verarbeitung ein hohes Risiko für die Rechte und Freiheiten der von der Datenverarbeitung betroffenen Personen - und somit die Notwendigkeit einer DSFA - mit sich bringt, umso größer wird, je mehr Kriterien bei der Verarbeitung erfüllt sind.

Verarbeitung mit einer neuen oder innovativen Technologie

In der Liste, die dem EDSA von der polnischen Aufsichtsbehörde zur Stellungnahme vorgelegt wurde, ist vorgesehen, dass für die Verarbeitung personenbezogener Daten mit einer innovative Technologie in Verbindung mit mindestens einem weiteren Kriterium eine DSFA erforderlich ist. Der EDSA nimmt zur Kenntnis, dass dieses Kriterium in der Liste aufgeführt ist.

3. Schlussfolgerungen und Empfehlungen

Da der von der polnischen Aufsichtsbehörde vorgelegte Listenentwurf zu einer inkohärenten Anwendung der Pflicht zur Durchführung einer DSFA führen könnte, sollte die Liste in folgenden Punkten geändert werden:

- indikativer Charakter der Liste: Der EDSA empfiehlt, in das Dokument mit der Liste einen Hinweis auf den nicht erschöpfenden Charakter der Liste einzufügen;
- Verweis auf die Leitlinien: Der EDSA empfiehlt der polnischen Aufsichtsbehörde, die Liste entsprechend zu ändern;
- biometrische Daten: Der EDSA empfiehlt der polnischen Aufsichtsbehörde, die Liste dahin gehend zu ändern, dass sie ausdrücklich um die Verarbeitung biometrischer Daten zur eindeutigen Identifizierung einer natürlichen Person in Verbindung mit mindestens einem weiteren auf der Liste aufgeführten Kriterium erweitert wird;
- genetische Daten: Der EDSA empfiehlt der polnischen Aufsichtsbehörde, die Liste dahin gehend zu ändern, dass sie ausdrücklich um die Verarbeitung genetischer Daten in Verbindung mit mindestens einem weiteren auf der Liste aufgeführten Kriterium erweitert wird;
- Standortdaten: Der EDSA empfiehlt der polnischen Aufsichtsbehörde, die in Verbindung mit einem weiteren Kriterium erfolgende Verarbeitung von Standortdaten in ihre Liste aufzunehmen;
- Überwachung am Arbeitsplatz: Diesbezüglich möchte der EDSA lediglich die Empfehlung hinzufügen, dass in Bezug auf die zwei Kriterien explizit auf die Leitlinien der Datenschutzgruppe nach Artikel 29 (WP248) verwiesen werden sollte.
- Abweichungen von den Leitlinien: Der EDSA empfiehlt der polnischen Aufsichtsbehörde, ihre Liste in Einklang mit den Leitlinien zu bringen, indem hinzugefügt wird, dass bei den vorgenannten Punkten eine DSFA in den meisten Fällen nur erforderlich ist, wenn bei der betreffenden Verarbeitung zwei Kriterien erfüllt sind.

4. Abschließende Bemerkungen

Diese Stellungnahme ist an die polnische Aufsichtsbehörde gerichtet und wird gemäß Artikel 64 Absatz 5 Buchstabe b DSGVO veröffentlicht.

Gemäß Artikel 64 Absätze 7 und 8 DSGVO hat die Aufsichtsbehörde dem Vorsitz binnen zwei Wochen nach Eingang der Stellungnahme auf elektronischem Wege mitzuteilen, ob sie den Listenentwurf beibehalten oder ändern wird. Innerhalb derselben Frist hat sie gegebenenfalls den geänderten Listenentwurf zu übermitteln, es sei denn, sie beabsichtigt, der Stellungnahme des EDSA insgesamt oder teilweise nicht zu folgen; in diesem Fall hat sie die maßgeblichen Gründe mitzuteilen.

Für den Europäischen Datenschutzausschuss

Die Vorsitzende

(Andrea Jelinek)