

Stellungnahme des EDSA nach Artikel 64 DSGVO



Stellungnahme des EDSA nach Artikel 64 DSGVO

Plenarsitzung des EDSA vom 4./5.12.2018

Stellungnahme 25/2018 zu der von der zuständigen Aufsichtsbehörde Kroatiens entworfenen Liste der Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist (Artikel 35 Absatz 4 DSGVO)

angenommen am 4. Dezember 2018

Translations proofread by EDPB Members.

This language version has not yet been proofread.

INHALT

1	Zusammenfassung des Sachverhalts.....	4
2	Bewertung.....	5
2.1	Allgemeine Anmerkungen des EDSA zu der eingereichten Liste	5
2.2	Anwendung des Kohärenzverfahrens auf den Listenentwurf	6
2.3	Analyse des Listenentwurfs	6
2.3.1	Verweis auf die Leitlinien.....	6
2.3.2	Biometrische Daten.....	6
2.3.3	Genetische Daten.....	7
2.3.4	Verarbeitung von Sensorvorrichtungen generierter personenbezogener Daten	7
3	Schlussfolgerungen und Empfehlungen.....	7
4	Abschließende Bemerkungen	8

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 sind², 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 am 5. September 2018 vom EDSA eine Stellungnahme zu ihren Listenentwürfen erhalten. Weitere vier zuständige Aufsichtsbehörden haben ihre Listenentwürfe Anfang Oktober eingereicht. Die Gesamtbewertung dieser Listenentwürfe dient dem Ziel einer kohärenten Anwendung der DSGVO, wengleich 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 ZUSAMMENFASSUNG DES SACHVERHALTS

1. Die Agentur für den Schutz personenbezogener Daten (im Folgenden „die kroatische Aufsichtsbehörde“) hat ihren Listenentwurf dem EDSA übermittelt. Der Beschluss über den Abschluss der Akte erging am 9. Oktober 2018.
Die Frist für die Annahme der Stellungnahme wurde angesichts der Komplexität der Angelegenheit

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.

sowie der Notwendigkeit, den Ergebnissen der Prüfung der zuvor von 22 zuständigen Aufsichtsbehörden eingereichten Listenentwürfe Rechnung zu tragen und eine Gesamtbewertung vorzunehmen, bis zum 16. Januar 2019 verlängert.

2 BEWERTUNG

2.1 Allgemeine Anmerkungen des EDSA zu der eingereichten Liste

2. 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.
3. 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.
4. Ferner sollte die kroatische 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.
5. In dieser Stellungnahme werden alle von der kroatischen 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.
6. 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.
7. In dieser Stellungnahme wird ein kohärenter Kern von Verarbeitungsvorgängen definiert, die auf allen von den Aufsichtsbehörden eingereichten Listen aufgeführt sind.
8. 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 empfohlen, ihre Listen entsprechend zu ändern, damit Kohärenz sichergestellt wird.
9. Wird in dieser Stellungnahme nicht auf Datenschutzfolgeabschätzungen eingegangen, die auf der eingereichten Liste aufgeführt sind, bedeutet dies, dass der EDSA der kroatischen Aufsichtsbehörde diesbezüglich keine weiteren Maßnahmen empfiehlt.

10. 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 kroatischen Aufsichtsbehörde bei der Aufstellung der Liste berücksichtigt wurden.

2.2 Anwendung des Kohärenzverfahrens auf den Listenentwurf

11. Der von der kroatischen Aufsichtsbehörde eingereichte Listenentwurf bezieht sich, da die auf ihm aufgeführten Verarbeitungsvorgänge nicht auf betroffene Personen in Kroatien 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

12. 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 DSGVO eine nicht erschöpfende Liste von Verarbeitungsvorgängen vorsieht, die eine DSFA erfordern,

gelangt der EDSA zu folgender Stellungnahme:

2.3.1 Verweis auf die Leitlinien

13. Nach dem Dafürhalten des EDSA ist die Analyse, die die Datenschutzgruppe nach Artikel 29 in ihren Leitlinien (WP248) 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.
14. Die kroatische Aufsichtsbehörde hat diesbezüglich angemerkt, man habe die Leitlinien zur DSFA ebenso analysiert wie die vorliegenden Unterlagen und Rechtsakte anderer mit dem Schutz personenbezogener Daten in der EU befasster Organe und Behörden. Da davon auszugehen ist, dass nicht alle Leser mit den von der Datenschutzgruppe nach Artikel 29 ausgearbeiteten Leitlinien zur Datenschutzfolgenabschätzung (WP 248) vertraut sind, empfiehlt der EDSA der kroatischen Aufsichtsbehörde, in ihrem Dokument klarzustellen, dass auf eben diese Leitlinien Bezug genommen wird. Der EDSA empfiehlt der kroatischen Aufsichtsbehörde zudem, in ihrem Dokument zu präzisieren, dass sich ihre Liste auf diese Leitlinien gründet, sie ergänzt und sie näher spezifiziert.

2.3.2 Biometrische Daten

15. In der Liste, die dem EDSA von der kroatischen Aufsichtsbehörde zur Stellungnahme vorgelegt wurde, ist angegeben, dass die Verarbeitung biometrischer Daten per se der Pflicht unterliegt, eine DSFA durchzuführen. Nach dem Dafürhalten des EDSA bringt die Verarbeitung biometrischer Daten

als solche nicht zwangsläufig ein hohes Risiko mit sich. Wenn die Verarbeitung biometrischer Daten zur eindeutigen Identifizierung einer natürlichen Person jedoch in Verbindung mit mindestens einem weiteren Kriterium erfolgt, ist eine DSFA erforderlich. Der EDSA empfiehlt der kroatischen Aufsichtsbehörde daher, die Liste unbeschadet von Artikel 35 Absatz 3 DSGVO dahin gehend zu ändern, dass bei dem Punkt, in dem die Verarbeitung biometrischer Daten zur eindeutigen Identifizierung einer natürlichen Person angesprochen wird, hinzugefügt wird, dass eine DSFA nur erforderlich ist, wenn diese Verarbeitung in Verbindung mit mindestens einem weiteren Kriterium erfolgt.

2.3.3 Genetische Daten

16. In der Liste, die dem EDSA von der kroatischen Aufsichtsbehörde zur Stellungnahme vorgelegt wurde, ist angegeben, dass die Verarbeitung genetischer Daten per se der Pflicht unterliegt, eine DSFA durchzuführen. 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 kroatischen Aufsichtsbehörde daher, die Liste unbeschadet von Artikel 35 Absatz 3 DSGVO dahin gehend zu ändern, dass bei dem Punkt, in dem die Verarbeitung genetischer Daten angesprochen wird, hinzugefügt wird, dass eine DSFA nur erforderlich ist, wenn diese Verarbeitung in Verbindung mit mindestens einem weiteren Kriterium erfolgt.

2.3.4 Verarbeitung von Sensorvorrichtungen generierter personenbezogener Daten

17. Nach dem Dafürhalten des EDSA sollte die Verarbeitung von Sensorvorrichtungen generierter und über das Internet oder mittels anderer Informationsübermittlungstechnologien übermittelter personenbezogener Daten weder allein noch in Verbindung mit einem anderen Kriterium ein die Pflicht zur Durchführung einer DSFA mit sich bringendes Kriterium sein, da sie nicht zwangsläufig ein hohes Risiko birgt. Nach Auffassung des EDSA geht der vorgelegte Listenentwurf, so wie er aktuell formuliert ist, in diesem Punkt zu weit. Da in der Liste, die dem EDSA von der kroatischen Aufsichtsbehörde zur Stellungnahme vorgelegt wurde, vorgesehen ist, dass für derartige Verarbeitungsvorgänge eine DSFA erforderlich ist, empfiehlt der EDSA der kroatischen Aufsichtsbehörde, diesen Punkt von ihrer Liste zu streichen.

3 SCHLUSSFOLGERUNGEN UND EMPFEHLUNGEN

18. Da der von der kroatischen Aufsichtsbehörde vorgelegte Listenentwurf zu einer inkohärenten Anwendung der Pflicht zur Durchführung einer DSFA führen könnte, sollte die Liste in folgenden Punkten geändert werden:
 -) Verweis auf die Leitlinien: Der EDSA empfiehlt der kroatischen Aufsichtsbehörde, in ihrem Dokument zu präzisieren, dass sich ihre Liste auf die Leitlinien gründet, sie ergänzt und sie näher spezifiziert;
 -) biometrische Daten: Der EDSA empfiehlt der kroatischen Aufsichtsbehörde, die Liste dahin gehend zu ändern, dass bei dem Punkt, in dem die Verarbeitung biometrischer Daten zur eindeutigen Identifizierung einer natürlichen Person angesprochen wird, hinzugefügt wird, dass eine DSFA nur erforderlich ist, wenn diese Verarbeitung in Verbindung mit mindestens einem weiteren Kriterium erfolgt;

-) genetische Daten: Der EDSA empfiehlt der kroatischen Aufsichtsbehörde, die Liste dahin gehend zu ändern, dass bei dem Punkt, in dem die Verarbeitung genetischer Daten angesprochen wird, hinzugefügt wird, dass eine DSFA nur erforderlich ist, wenn diese Verarbeitung in Verbindung mit mindestens einem weiteren Kriterium erfolgt;
-) Verarbeitung von Sensorvorrichtungen generierter personenbezogener Daten: Der EDSA empfiehlt der kroatischen Aufsichtsbehörde, diesen Punkt von ihrer Liste zu streichen.

4 ABSCHLIEßENDE BEMERKUNGEN

19. Diese Stellungnahme ist an die kroatische Aufsichtsbehörde gerichtet und wird gemäß Artikel 64 Absatz 5 Buchstabe b DSGVO veröffentlicht.
20. 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)