Empfehlung 01/2019 zu der vom Europäischen Datenschutzbeauftragten entworfenen Liste der Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist (Artikel 39 Absatz 4 der Verordnung (EU) 2018/1725)

angenommen am 10. Juli 2019

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Inhalt

Der Europäische Datenschutzausschuss —

gestützt auf Artikel 70 Absatz 1 Buchstabe e 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 Artikel 39 Absatz 4 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG (im Folgenden „Verordnung 2018/1725“),

gestützt auf die Artikel 12 und 22 seiner Geschäftsordnung vom 25. Mai 2018 in der überarbeiteten Fassung vom 23. November 2018,

in Erwägung nachstehender Gründe:

(1) Die Hauptaufgabe des Ausschusses besteht darin, eine kohärente Anwendung der DSGVO im gesamten Europäischen Wirtschaftsraum sicherzustellen. Zu diesem Zweck prüft der Ausschuss gemäß Artikel 70 Absatz 1 Buchstabe e DSGVO auf Antrag eines seiner Mitglieder etwaige die Anwendung dieser Verordnung betreffenden Fragen und stellt Leitlinien, Empfehlungen und bewährte Verfahren bereit, um die einheitliche Anwendung dieser Verordnung sicherzustellen. Artikel 39 Absatz 6 der Verordnung (EU) 2018/1725 sieht vor, dass der Europäische Datenschutzbeauftragte dem EDSA gemäß Artikel 70 Absatz 1 Buchstabe e DSGVO den Entwurf einer Liste der Verarbeitungsvorgänge, für die gemäß Artikel 39 Absatz 4 der Verordnung (EU) 2018/1725 eine Datenschutz-Folgenabschätzung (DSFA) durchzuführen ist, vor deren Festlegung zur Prüfung vorlegt. Diese Pflicht gilt für jede Liste, die sich auf Verarbeitungsvorgänge eines Verantwortlichen im Sinne von Artikel 3 Absatz 8 der Verordnung (EU) 2018/1725 bezieht, der gemeinsam mit einem oder mehreren Verantwortlichen, die nicht Organe oder Einrichtungen der Union sind, tätig ist. Diese Empfehlung stellt daher auf eine Vorgehensweise ab, die mit dem unlängst bei den Listenentwürfen der Aufsichtsbehörden verfolgten Ansatz kohärent ist. Um ein einheitliches Vorgehen sicherzustellen, hat der Ausschuss den Aufsichtsbehörden in seinen Stellungnahmen jeweils empfohlen, 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.

(4) Gemäß Artikel 39 Absatz 1 der Verordnung (EU) 2018/1725 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 39 Absatz 3 der Verordnung (EU) 2018/1725 sind exemplarisch mehrere Fälle genannt, in denen ein solches hohes Risiko bestehen kann. Dabei handelt es sich um eine nicht erschöpfende Aufzählung von Fällen, die sich wörtlich mit der Aufzählung in Artikel 35 Absatz 3 DSGVO deckt. 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 vom Europäischen Datenschutzbeauftragten 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 sind hierfür relevant —

HAT FOLGENDE EMPFEHLUNG ERLASSEN:

1 ZUSAMMENFASSUNG DES SACHVERHALTS

1. Der Europäische Datenschutzbeauftragte hat dem EDSA am 18. März 2019 seinen Listenentwurf in Anwendung von Artikel 39 Absatz 4 der Verordnung (EU) 2018/1725 vorgelegt und dem EDSA am 21. Juni 2019 eine überarbeitete Fassung übermittelt.

2. Der vom Europäischen Datenschutzbeauftragten vorgelegte Listenentwurf enthält auch einen Teil, der sich auf Artikel 39 Absatz 5 der Verordnung (EU) 2018/1725 bezieht. In dem überarbeiteten Entwurf wird ausdrücklich darauf hingewiesen, dass der sich auf Artikel 39 Absatz 5 beziehende Listenteil nur für Situationen gilt, in denen Organe oder Einrichtungen der Union gemeinsame oder alleinige Verantwortliche sind. Konkret werden in dem sich auf Artikel 39 Absatz 5 beziehenden Listenteil Verarbeitungsvorgänge angeführt, die im Zusammenhang mit Datenverarbeitungen der Organe oder Einrichtungen der Union für deren interne Verwaltung stehen und an denen neben den Organen oder Einrichtungen der Union keine weiteren Verantwortlichen beteiligt sind.

3. Diesbezüglich stellt der EDSA fest, dass dieser zweite Listenteil nicht in den Anwendungsbereich von Artikel 39 Absatz 6 der Verordnung (EU) 2018/1725 fällt. Dort ist nämlich vorgesehen, dass die Pflicht, dem EDSA einen Listenentwurf zur Prüfung vorzulegen, nur für Verarbeitungsvorgänge eines den Bestimmungen der Verordnung (EU) 2018/1725 unterliegenden Verantwortlichen gilt, der gemeinsam mit einem oder mehreren Verantwortlichen, die nicht Organe oder Einrichtungen der Union sind, tätig ist. Daher wird der EDSA auf diesen Teil des Listenentwurfs nicht weiter eingehen.

2 BEURTEILUNG

2.1 Allgemeine Anmerkungen des EDSA zu der eingereichten Liste

[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.

4. Die dem EDSA vorgelegte Liste wird als nähere Spezifizierung von Artikel 39 Absatz 1 der Verordnung (EU) 2018/1725 ausgelegt, der in jedem Fall maßgeblich bleiben wird. Die Liste sollte daher nicht als erschöpfend betrachtet werden.

5. Der EDSA nimmt zur Kenntnis, dass in Artikel 39 Absatz 10 der Verordnung (EU) 2018/1725 festgelegt ist, dass keine DSFA erforderlich ist, wenn der konkrete Verarbeitungsvorgang oder die konkreten Verarbeitungsvorgänge auf einem auf der Grundlage der Verträge erlassenen Rechtsakt beruhen und bereits im Rahmen der allgemeinen Folgenabschätzung vor Erlass dieses Rechtsakts eine Datenschutz-Folgenabschätzung erfolgt ist. In diesem Fall gilt Artikel 39 Absätze 1 bis 6 nicht, sofern in dem genannten Rechtsakt nichts anderes bestimmt ist.

6. Auf im Listenentwurf des Europäischen Datenschutzbeauftragten aufgeführte Kategorien von Verarbeitungstätigkeiten, die nach dem Dafürhalten des EDSA nicht in den Anwendungsbereich von Artikel 39 Absatz 6 der Verordnung (EU) 2018/1725 fallen, wird in dieser Empfehlung nicht generell eingegangen. Dabei handelt es sich um Kategorien von Verarbeitungstätigkeiten, die keine Verarbeitungen betreffen, welche durch Verantwortliche erfolgen, die gemeinsam mit einem oder mehreren Verantwortlichen, welche nicht Organe oder Einrichtungen der Union sind, tätig sind. Da der Europäische Datenschutzbeauftragte jedoch beschlossen hat, eine gemeinsame Liste für beide Arten von Verarbeitungsvorgängen anzunehmen, gilt die vorliegende Empfehlung de facto für beide Kategorien von Verarbeitungstätigkeiten.

7. Die Empfehlung bezweckt ein einheitliches Vorgehen, das sich mit der Vorgehensweise in Bezug auf den Kern der Verarbeitungsvorgänge deckt, um deren Aufnahme in die Listen der Aufsichtsbehörden (sofern nicht bereits vorhanden) der EDSA die Aufsichtsbehörden ersucht hat.

8. Der EDSA empfiehlt dem Europäischen Datenschutzbeauftragten daher, für die begrenzte Zahl von Verarbeitungsvorgängen, für die der EDSA eine einheitliche Definition festlegt, eine DSFA vorzuschreiben.

9. Wird in dieser Empfehlung nicht auf Datenschutzfolgeabschätzungen eingegangen, die auf der eingereichten Liste aufgeführt sind, bedeutet dies, dass der EDSA dem Europäischen Datenschutzbeauftragten 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. Um diese Transparenz zu verbessern, empfiehlt der EDSA, bei jedem auf der Liste aufgeführten Verarbeitungsvorgang zur näheren Präzisierung explizit auf die betreffenden Kriterien der Leitlinien zu verweisen.

2.2 Analyse des Listenentwurfs

11. Unter Berücksichtigung der Tatsache, dass

a. Artikel 39 Absatz 1 der Verordnung (EU) 2018/1725 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 39 Absatz 3 der Verordnung (EU) 2018/1725 eine nicht erschöpfende Liste von Verarbeitungsvorgängen vorsieht, die eine DSFA erfordern,

spricht der EDSA folgende Empfehlungen aus:

SENSIBLE DATEN

12. In dem Listenentwurf werden folgende sensible Daten als Kriterium für die Notwendigkeit einer DSFA genannt: „personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten über das Sexualleben oder die sexuelle Orientierung einer natürlichen Person, personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln oder anderweitig für sensibel befundene Daten“.

13. Diese Aufzählung ähnelt zwar sehr der in den vom EDSA gebilligten, ursprünglich von der Datenschutzgruppe nach Artikel 29 verfassten Leitlinien zur Datenschutz-Folgenabschätzung (WP248rev.01), weist aber einen entscheidenden Unterschied auf: Während es in den Leitlinien heißt: „vertrauliche Daten oder höchst persönliche Daten“, spricht der Listenentwurf von „anderweitig für sensibel befundenen Daten“.

14. Der EDSA weist darauf hin, dass der Begriff „sensible Daten“ in der DSGVO lediglich in zwei Erwägungsgründen, aber in keinem Artikel erwähnt wird. Gleichwohl geht er davon aus, dass dieser Begriff ausschließlich die in den Artikeln 9 und 10 DSGVO genannten Datenkategorien umfasst. Damit keine Verwirrung entsteht, empfiehlt der EDSA dem Europäischen Datenschutzbeauftragten, anstelle der Formulierung „oder anderweitig für sensibel befundene Daten“ die besagte Formulierung aus den Leitlinien zur Datenschutz-Folgenabschätzung zu verwenden.

UMFANGREICHE VERARBEITUNG

15. Der EDSA stellt fest, dass der Europäische Datenschutzbeauftragte das interne Telefonverzeichnis eines EU-Organs als negatives Beispiel für eine umfangreiche Verarbeitung anführt. Ungeachtet der Frage, ob in diesem Fall tatsächlich eine DSFA erforderlich ist, ist hier jedoch nicht klar, warum ein Telefonverzeichnis eines EU-Organs nicht per se unter den Begriff „umfangreiche Verarbeitung“ fallen sollte, zumal es ja personenbezogene Daten einer Vielzahl von Einzelpersonen enthalten kann. Der EDSA erinnert zudem daran, dass der Begriff „umfangreich“ auch in Verbindung mit dem betroffenen Bevölkerungsanteil verwendet wird - siehe Definition in den vom EDSA gebilligten Leitlinien zu Datenschutzbeauftragten, die im Dezember 2016 angenommen und am 5. April 2017 überarbeitet wurden. Der EDSA empfiehlt daher, ein anderes Beispiel zu nennen.

DATENSÄTZE, DIE AUF DER GRUNDLAGE UNTERSCHIEDLICHER DATENVERARBEITUNGSVORGÄNGE EINANDER ZUGEORDNET ODER MITEINANDER KOMBINIERT WERDEN

16. Der EDSA stellt fest, dass bei dem Beispiel, das für Verarbeitungsvorgänge genannt wird, bei denen Datensätze verwendet werden, die auf der Grundlage unterschiedlicher Datenverarbeitungsvorgänge einander zugeordnet oder miteinander kombiniert werden, so wie es beschrieben ist, Zweifel an seiner Zulässigkeit nach der Verordnung (EU) 2018/1725 aufkommen könnten. Der EDSA verfügt nicht über die nötige Stellung und Befugnis, um die Frage der Zulässigkeit prüfen zu können. Der Klarheit halber empfiehlt er jedoch, auf ein anderes Beispiel zurückzugreifen.

SCHUTZBEDÜRFTIGE BETROFFENE PERSONEN

17. Der EDSA stellt fest, dass der Europäische Datenschutzbeauftragte in seinem Listenentwurf als negatives Beispiel die Stellung der Bediensteten der EU-Organe im Rahmen der im Statut festgelegten Standardverfahren anführt. Der EDSA erinnert daran, dass in den vom EDSA gebilligten, ursprünglich von der Datenschutzgruppe nach Artikel 29 verfassten Leitlinien zur Datenschutz-Folgenabschätzung (WP248rev.01) „Angestellte" als schutzbedürftige betroffene Personen eingestuft werden. Zwar lässt sich argumentieren, dass das ungleiche Kräfteverhältnis zwischen Arbeitgeber und Arbeitnehmer bei den Standardverfahren nach den einschlägigen Vorschriften des Statuts weniger stark ausgeprägt ist, doch kann keineswegs davon ausgegangen werden, dass dies immer der Fall ist. Dies gilt besonders dann, wenn die Bediensteten keinen maßgeblichen Einfluss auf den Inhalt des besagten Statuts nehmen können. Auch ist nicht klar, welche Verfahren als nicht standardgemäß zu betrachten sind und dementsprechend eine DSFA erforderlich machen können - was zu erheblicher Verwirrung führen könnte. Aus diesen Gründen empfiehlt der EDSA dem Europäischen Datenschutzbeauftragten, das von ihm angeführte negative Beispiel durch ein anderes zu ersetzen.

3 SCHLUSSFOLGERUNG

18. Der EDSA empfiehlt dem Europäischen Datenschutzbeauftragten, seinen Listenentwurf wie folgt zu ändern:

- sensible Daten: Der EDSA empfiehlt dem Europäischen Datenschutzbeauftragten, anstelle der Formulierung „oder anderweitig für sensibel befundene Daten" die genaue Formulierung aus den Leitlinien zur Datenschutz-Folgenabschätzung zu verwenden;
- umfangreiche Verarbeitung: Der EDSA empfiehlt dem Europäischen Datenschutzbeauftragten, das diesbezüglich angeführte negative Beispiel durch ein anderes zu ersetzen;
- Datensätze, die auf der Grundlage unterschiedlicher Datenverarbeitungsvorgänge einander zugeordnet oder miteinander kombiniert werden: Der EDSA empfiehlt dem Europäischen Datenschutzbeauftragten, das diesbezüglich angeführte negative Beispiel durch ein anderes zu ersetzen;
- schutzbedürftige betroffene Personen: Der EDSA empfiehlt dem Europäischen Datenschutzbeauftragten, das diesbezüglich angeführte negative Beispiel durch ein anderes zu ersetzen.

Für den Europäischen Datenschutzausschuss

Die Vorsitzende

(Andrea Jelinek)