



Liste von Verarbeitungsvorgängen nach Art. 35 Abs. 4 DS-GVO

für die gemäß Art. 35 Abs. 1 DS-GVO eine Datenschutz-Folgenabschätzung
von Verantwortlichen im öffentlichen Bereich durchzuführen ist

A Gesetzliche Grundlage

Die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates (EU-Datenschutz-Grundverordnung – DS-GVO) regelt im Abschnitt 3 „Datenschutz-Folgenabschätzung und vorherige Konsultation“ des Kapitels IV „Verantwortlicher und Auftragsverarbeiter“ die Rahmenbedingungen zur sog. Datenschutz-Folgenabschätzung (kurz: DSFA; im Englischen Data Protection Impact Assessment oder DPIA). Artikel 35 DS-GVO nennt dabei die Grundsätze, bei welchen Fällen eine DSFA durchzuführen ist und was diese enthält. Artikel 36 DS-GVO beschreibt das besondere Verfahren der Konsultation des Verantwortlichen bei der Aufsichtsbehörde bei Fortbestehen hoher Risiken auch nach Anwendung der auf Grundlage der DSFA festgelegten verhältnismäßigen technischen und organisatorischen Maßnahmen.

Grundlage dieses Dokuments ist Art. 35 Abs. 4 DS-GVO:

„Die Aufsichtsbehörde erstellt eine Liste der Verarbeitungsvorgänge, für die gemäß Absatz 1 eine Datenschutz-Folgenabschätzung durchzuführen ist, und veröffentlicht diese. Die Aufsichtsbehörde übermittelt diese Listen dem in Artikel 68 genannten Ausschuss.“

Die vorliegende Liste beinhaltet ausschließlich Verarbeitungsvorgänge aus dem öffentlichen Bereich. Die in dem Dokument dargestellte Liste wird nachfolgend als „Muss-Liste“ bezeichnet – gängige Begriffe in anderen Ländern sind hierfür auch „Blacklist“ und „Positivliste“.

B Ziel dieses Dokuments

Ziel des Dokuments ist eine Liste nach Art. 35 Abs. 4 DS-GVO, die auch auf europäischer Ebene diskutiert werden kann. Berücksichtigt werden bisherige Veröffentlichungen von anderen Aufsichtsbehörden und Fachgremien, insbesondere das Working Paper 248 rev.01 „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““ der Art. 29 Datenschutzgruppe sowie die umfangreichen internen Kommentierungen im Rahmen der UAG DSFA.

Das Dokument hat nicht den Anspruch der Vollständigkeit, wenngleich versucht wird, möglichst viele der DSFA-pflichtigen Verarbeitungsvorgänge zu berücksichtigen. Auf Grund der Schnellebigkeit im digitalen Umfeld kann dieses Dokument nur als „lebendiges“ Papier angesehen werden, das ständigen Änderungskontrollen hinsichtlich der Aufnahme neuer Verarbeitungen in die Liste der Verarbeitungsvorgänge unterliegt.

Wichtiger Hinweis:

Wird die Verarbeitungstätigkeit eines Verantwortlichen in der vorliegenden Liste nicht aufgeführt, so ist hieraus nicht der Schluss zu ziehen, dass keine DSFA durchzuführen wäre. Stattdessen ist es Aufgabe des Verantwortlichen, im Wege einer Vorabprüfung einzuschätzen, ob die Verarbeitung aufgrund ihrer Art, ihres Umfangs, ihrer Umstände und ihrer Zwecke voraussichtlich ein **hohes Risiko** für die Rechte und Freiheiten natürlicher Personen aufweist und damit die Voraussetzungen des Art. 35 Abs. 1 Satz 1 DS-GVO erfüllt. Zum Begriff des Risikos wird auf die 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 17/DE angenommen am 4. April 2017, zuletzt überarbeitet und angenommen am 4. Oktober 2017) der Art. 29 Datenschutzgruppe und das Kurzpapier Nr. 18 „Risiken für die Rechte und Freiheiten natürlicher Personen“ der DSK verwiesen.

C Liste nach Art. 35 Abs. 4 DS-GVO

Maßgebliche Kriterien zur Einordnung von Verarbeitungsvorgängen sind in der Leitlinie in WP 248 der Art. 29 Gruppe ab Seite 10 ff. wie folgt zu entnehmen:

1. Bewerten oder Einstufen (Scoring)
(“Evaluation or scoring”)
2. Automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung
(“Automated-decision making with legal or similar significant effect”)
3. Systematische Überwachung
(“Systematic monitoring”)
4. Vertrauliche oder höchst persönliche Daten
(“Sensitive data or data of a highly personal nature”)
5. Datenverarbeitung in großem Umfang
(“Data processed on a large scale”)
6. Abgleichen oder Zusammenführen von Datensätzen
(“Matching or combining datasets”)
7. Daten zu schutzbedürftigen Betroffenen
(“Data concerning vulnerable data subjects”)
8. Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen
(“Innovative use or applying new technological or organisational solutions”)
9. Betroffene werden an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags gehindert
(“When the processing in itself prevents data subjects from exercising a right or using a service or a contract”)

Erfüllt ein Verarbeitungsvorgang zwei oder mehr dieser Kriterien, so ist vielfach ein hohes Risiko gegeben und eine DSFA durch den Verantwortlichen durchzuführen. In wenigen Einzelfällen mag es jedoch auch vorkommen, dass nur eines der genannten Kriterien erfüllt wird und dennoch auf Grund eines hohen Risikos des Verarbeitungsvorgangs eine DSFA notwendig wird.

Das Ergebnis der Vorabprüfung und die zugrunde gelegten Einschätzungen der im Zuge der Verarbeitungstätigkeit möglicherweise auftretenden Schäden sowie die resultierende Schwere und Eintrittswahrscheinlichkeit der Risiken sind zu dokumentieren.

D Liste der Verarbeitungstätigkeiten, für die eine Datenschutz-Folgenabschätzung durchzuführen ist

Folgende Formen der Verarbeitung personenbezogener Daten durch Behörden und andere öffentliche Stellen, die nicht am Wettbewerb teilnehmen, unterliegen der Pflicht zur Erstellung einer Datenschutz-Folgenabschätzung gemäß Art. 35 Abs. 1 DSGVO:

Maßgebliche Definition
Die umfangreiche Verarbeitung von Daten, die dem <i>Sozial-, einem Berufs- oder besonderen Amtsgeheimnis</i> unterliegen, auch wenn es sich nicht um Daten gemäß Art. 9 Abs. 1 und 10 DSGVO handelt
Die Verarbeitung von Daten gemäß Art. 9 Abs. 1 und 10 DSGVO und von anderen Daten, die dem Sozial-, einem Berufs- oder besonderen Amtsgeheimnis unterliegen, soweit sie <ul style="list-style-type: none"> • durch verschiedene Stellen unter gemeinsamer Verantwortung gemäß Art. 26 DSGVO erfolgt, • die Übermittlung derartiger Daten auf automatisierten Abruf seitens einer anderen Stelle involviert oder einem anderen Zweck als demjenigen dient, zu dem die Daten erhoben wurden
Die Verarbeitung von Daten gemäß Art. 9 Abs. 1 und 10 DSGVO und von anderen Daten, die dem Sozial-, einem Berufs- oder besonderen Amtsgeheimnis unterliegen, durch Auftragsverarbeiter, denen von einem Gericht oder einer Verwaltungsbehörde eines Drittlands die Pflicht auferlegt werden kann, diese Daten entgegen Art. 48 DSGVO zu exportieren oder offenzulegen
Die Datenverarbeitung der Personenstands- und Melderegister sowie anderer Stellen, die Daten aus diesen Registern in großem Umfang, Meldedaten mit Sperrvermerken gemäß § 51 Abs. 1 und 5 Bundesmeldegesetz oder Personenstandsdaten gemäß § 63 Personenstandsgesetz verarbeiten
Die umfangreiche Verarbeitung von Daten über Kinder
Die umfangreiche Verarbeitung von Daten über den Aufenthaltsort von Personen
Die Zusammenführung von personenbezogenen Daten aus verschiedenen Quellen und Weiterverarbeitung der so zusammengeführten Daten, sofern <ul style="list-style-type: none"> • die Zusammenführung oder Weiterverarbeitung in großem Umfang vorgenommen werden, • für Zwecke erfolgen, für welche nicht alle der zu verarbeitenden Daten direkt bei den Betroffenen erhoben wurden, • die Anwendung von Algorithmen einschließen, die für die Betroffenen nicht nachvollziehbar sind, und der Erzeugung von Datengrundlagen dienen, die dazu genutzt werden können, Entscheidungen zu treffen, die Rechtswirkung gegenüber den betroffenen Personen entfalten, oder diese in ähnlich erheblicher Weise beeinträchtigen können
Die Zusammenführung von personenbezogenen Daten aus verschiedenen Quellen und der Weiterverarbeitung der so zusammengeführten Daten, sofern <ul style="list-style-type: none"> • die Zusammenführung oder Weiterverarbeitung in großem Umfang vorgenommen werden, • für Zwecke erfolgen, für welche nicht alle der zu verarbeitenden Daten direkt bei den Betroffenen erhoben wurden, • die Anwendung von Algorithmen einschließen, die für die Betroffenen nicht nachvollziehbar sind, und der Entdeckung vorher unbekannter Zusammenhänge zwischen den Daten für nicht im Vorhinein bestimmte Zwecke dienen
Die Erfassung und Veröffentlichung von Daten, die zur Bewertung des Verhaltens und anderer persönli-

cher Aspekte von Personen dienen und von Dritten dazu genutzt werden können, Entscheidungen zu treffen, die Rechtswirkung gegenüber den bewerteten Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen
Die Verarbeitung von umfangreichen Angaben über das Verhalten von <i>Beschäftigten</i> , die zur Bewertung ihrer Arbeitstätigkeit derart eingesetzt werden können, dass sich Rechtsfolgen für die Betroffenen ergeben, oder diese in andere Weise erheblich beeinträchtigen
Die Verarbeitung von Daten gemäß Art. 9 Abs. 1 und Art. 10 DSGVO - auch wenn sie nicht als „umfangreich“ im Sinne des Art 35 Abs. 3 lit. b) anzusehen ist - sofern die Daten dazu verwendet werden, die Leistungsfähigkeit von <i>Beschäftigten</i> zu bestimmen
Der Einsatz von <i>künstlicher Intelligenz</i> zur Verarbeitung personenbezogener Daten zur Steuerung der Interaktion mit den Betroffenen oder zur Bewertung persönlicher Aspekte der Betroffenen
Die mobile und für die Betroffenen intransparente <i>optoelektronische Erfassung</i> öffentlicher Bereiche
Die nicht bestimmungsgemäße Nutzung von Sensoren eines <i>Mobilfunkgeräts</i> im Besitz der Betroffenen oder von Funksignalen, die von solchen Geräten versandt werden, zur <i>Bestimmung des Aufenthaltsorts</i> oder der Bewegung von Personen über einen substantiellen Zeitraum und nachfolgende zentralisierte Verarbeitung der resultierenden Angaben
Die umfangreiche Erhebung personenbezogener Daten über Schnittstellen <i>persönlicher elektronischer Geräte</i> , die nicht gegen ein unbefugtes Auslesen geschützt sind, soweit diese Erhebung für die Betroffenen nicht erkennbar ist
Die automatisierte Auswertung von Video- oder Audio-Aufnahmen zur Bewertung der Persönlichkeit der Betroffenen