



Liste von Verarbeitungsvorgängen nach Art. 35 Abs. 4 DSGVO,

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

A Gesetzliche Grundlage

Die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates (EU-Datenschutz-Grundverordnung – DSGVO) 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 DSGVO:

„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 nicht mit dem Angebot von Waren und Dienstleistungen für betroffene Personen oder der Beobachtung des Verhaltens von natürlichen Personen in mehreren Mitgliedsstaaten verbunden sind. Sie unterliegt daher aufgrund von Art. 35 Abs. 6 DSGVO nicht dem Kohärenzverfahren gemäß Art. 63 DSGVO.

Führt ein Verantwortlicher Verarbeitungsvorgänge aus, die in Art. 35 Abs. 3 DSGVO (s.u.) oder der auf Seite 5 beginnenden Liste aufgeführt sind, ohne vorab eine DSFA durchgeführt zu haben, so kann die zuständige Aufsichtsbehörde wegen Verstoßes gegen Art. 35 Abs. 1 DSGVO von ihren Abhilfebefugnissen gemäß Art. 58 Abs. 2 DSGVO Gebrauch machen. Gegen einen derartigen Beschluss der Aufsichtsbehörde steht der Rechtsweg gemäß Art. 78 DSGVO offen.

Die vorliegende Liste findet auf Verarbeitungen personenbezogener Daten für die Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, sowie auf die Führung von Papier-Akten oder Aktensammlungen, die nicht nach bestimmten Kriterien geordnet sind, keine Anwendung.

B Gesetzlich unmittelbar vorgeschriebene DSFA-Pflicht

Eine Datenschutz-Folgenabschätzung ist gemäß Art. 35 Abs. 3 DSGVO stets in folgenden Fällen durchzuführen:

- a) bei systematischer und umfassender Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen;

- b) bei umfangreicher Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 DSGVO oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 DSGVO und
- c) bei systematischer umfangreicher Überwachung öffentlich zugänglicher Bereiche.

Die Größe des Umfangs der Verarbeitung bezieht sich sowohl auf die Zahl der Betroffenen, als auch den Umfang der Angaben zu jeder bzw. jedem einzelnen Betroffenen. Falls die Verarbeitung flächendeckend operiert, d. h. alle in Hamburg oder dem Zuständigkeitsbereich der jeweiligen Behörde lebenden oder sich dort aufhaltenden Personen erfasst, die ein bestimmtes Kriterium erfüllen, z. B. alle Kinder bis neun Jahren oder alle Personen mit hochinfektiösen Krankheiten aus einer vorgegebenen Liste, so ist stets davon auszugehen, dass es sich um eine umfangreiche Verarbeitung handelt.

Die Regelung nach Buchstabe b findet insbesondere bei Verarbeitungstätigkeiten von Behörden Anwendung, die gemäß ihrer Aufgabe

1. Daten, aus denen die rassische und ethnische Herkunft,
2. politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder
3. die Gewerkschaftszugehörigkeit hervorgehen,
4. genetische Daten,
5. biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person,
6. Gesundheitsdaten
7. Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person oder
8. Daten über strafrechtliche Verurteilungen und Straftaten

in großem Umfang verarbeiten.

Die Pflicht zur Durchführung von Datenschutz-Folgenabschätzungen trifft öffentliche Stellen, wenn sie Verarbeitungstätigkeiten vornehmen, die eine der oben genannten Bedingungen erfüllen, von der auf Seite 5 beginnenden Liste erfasst sind oder bei denen der Verantwortliche im Zuge einer Einzelabwägung zu dem Ergebnis gekommen ist, dass sie ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen i. S. v. Art. 35 Abs.1 DSGVO mit sich bringen.

Wird die Verarbeitungstätigkeit eines Verantwortlichen in der Liste ab Seite 5 nicht aufgeführt, so ist hieraus nicht der Schluss zu ziehen, dass keine Datenschutz-Folgenabschätzung 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 DSGVO 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“ der Art. 29 Datenschutzgruppe und das Kurzpapier Nr. 10 Risiken für die Rechte und Freiheiten natürlicher Personen der DSK verwiesen.

C Liste nach Art. 35 Abs. 4 DSGVO

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")

Die hier nur summarisch bezeichneten Kriterien werden in der Leitlinie näher erläutert.

Erfüllt ein Verarbeitungsvorgang zwei oder mehr dieser Kriterien, so ist in den meisten Fällen eine DSFA durch den Verantwortlichen durchzuführen. In wenigen Einzelfällen mag es 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.

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 Erstellung¹ einer Datenschutz-Folgenabschätzung gemäß Art. 35 Abs. 1 DSGVO:

Maßgebliche Definition

Umfangreiche Verarbeitung von Daten, die dem *Sozial-*, einem *Berufs-* oder *besonderen Amtsgeheimnis* unterliegen, auch wenn es sich nicht um Daten gemäß Art. 9 Abs. 1 und 10 DSGVO handelt

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

- 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

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

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

Umfangreiche Verarbeitung von Daten über Kinder

Umfangreiche Verarbeitung von Daten über den Aufenthaltsort von Personen

Zusammenführung von personenbezogenen Daten aus verschiedenen Quellen und Weiterverarbeitung der so zusammengeführten Daten, sofern

- 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

¹ Für Verarbeitungstätigkeiten, die nicht in der Liste aufgeführt sind, sind die Ausführungen auf Seite 3, letzter Absatz zu beachten.

zu treffen, die Rechtswirkung gegenüber den betroffenen Personen entfalten, oder diese in ähnlich erheblicher Weise beeinträchtigen können

Zusammenführung von personenbezogenen Daten aus verschiedenen Quellen und der Weiterverarbeitung der so zusammengeführten Daten, sofern

- 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

Erfassung und Veröffentlichung von Daten, die zur Bewertung des Verhaltens und anderer persönlicher 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

Verarbeitung von umfangreichen Angaben über das Verhalten von *Beschäftigten*, die zur Bewertung ihrer Arbeitstätigkeit derart eingesetzt werden können, dass sich Rechtsfolgen für die Betroffenen ergeben, oder diese in andere Weise erheblich beeinträchtigen

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 *Beschäftigten* zu bestimmen

Der Einsatz von *künstlicher Intelligenz* zur Verarbeitung personenbezogener Daten zur Steuerung der Interaktion mit den Betroffenen oder zur Bewertung persönlicher Aspekte der Betroffenen

Mobile und für die Betroffenen intransparente *optoelektronische Erfassung* öffentlicher Bereiche

Nicht bestimmungsgemäße Nutzung von Sensoren eines *Mobilfunkgeräts* im Besitz der Betroffenen oder von Funksignalen, die von solchen Geräten versandt werden, zur *Bestimmung des Aufenthaltsorts* oder der Bewegung von Personen über einen substantiellen Zeitraum und nachfolgende zentralisierte Verarbeitung der resultierenden Angaben

Umfangreiche Erhebung personenbezogener Daten über Schnittstellen *persönlicher elektronischer Geräte*, die nicht gegen ein unbefugtes Auslesen geschützt sind, soweit diese Erhebung für die Betroffenen nicht erkennbar ist

Automatisierte Auswertung von Video- oder Audio-Aufnahmen zur Bewertung der Persönlichkeit der Betroffenen