Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

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 nicht-öffentlichen Bereich** durchzuführen ist

Version 1.1
Stand: 17.10.2018

Die im vorliegenden Text enthaltene Liste wurde von den Mitgliedern der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder am 15.10.2018 einvernehmlich angenommen. Sie folgt der gemäß Art. 64 Abs. 3 Datenschutz-Grundverordnung abgegebenen Stellungnahme des Europäischen Datenschutzausschusses 05/2018 vom 25.09.2018.

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 (DSFA). 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 der Aufsichtsbehörde durch den Verantwortlichen 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."

Führt ein Verantwortlicher Verarbeitungsvorgänge aus, für die gemäß Art. 35 Abs.1 DS-GVO eine DSFA durchzuführen ist, ohne dass er dieser Pflicht genüge getan hat, so kann die zuständige Aufsichtsbehörde wegen Verstoßes gegen Art. 35 Abs. 1 DS-GVO von ihren Abhilfebefugnissen gemäß Art. 58 Abs. 2 DS-GVO einschließlich der Verhängung von Geldbußen gemäß Art. 83 Abs. 4 DS-GVO Gebrauch machen. Gegen einen derartigen Beschluss der Aufsichtsbehörde steht der Rechtsweg gemäß Art. 78 DS-GVO offen.

B Gesetzlich unmittelbar vorgeschriebene DSFA-Pflicht

Eine Datenschutz-Folgenabschätzung ist gemäß Art. 35 Abs. 3 DS-GVO 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 DS-GVO oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 DS-GVO 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.

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

Eine Datenschutz-Folgenabschätzung gemäß Art. 35 Abs. 1 DS-GVO ist durchzuführen, falls die geplante Verarbeitungstätigkeit die in der zweiten Spalte der folgenden Tabelle aufgeführten Merkmale aufweist.

In der dritten Spalte sind typische Einsatzfelder von derartigen Datenverarbeitungsvorgängen aufgeführt. Die Aufzählung ist weder abschließend noch maßgeblich, sondern dient lediglich dazu, typischen Verarbeitern zu helfen, sie betreffende Einträge aufzufinden. Datenschutz-Folgenabschätzungen sind auch bei Verarbeitungstätigkeiten außerhalb der genannten Einsatzfelder durchzuführen, falls sie die maßgeblichen Kriterien in der zweiten Spalte erfüllen. Die vierte Spalte dient lediglich der Illustration.

Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist

Nr.	Maßgebliche Beschreibung der Verarbeitungstätigkeit	Typische Einsatzfelder	Beispiele
1	Verarbeitung von biometrischen Daten zur eindeutigen Identifizierung natürlicher Personen, wenn mindestens ein weiteres folgendes Kriterium aus WP 248 Rev. 01 zutrifft: ▪ Daten zu schutzbedürftigen Betroffenen ▪ Systematische Überwachung ▪ Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen ▪ Bewerten oder Einstufen (Scoring) ▪ Abgleichen oder Zusammenführen von Datensätzen ▪ Automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung ▪ Betroffene werden an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags gehindert	Verwendung von biometrischen Systemen zur Zutrittskontrolle oder für Abrechnungszwecke.	Ein Unternehmen setzt flächendeckend Fingerabdrucksensoren zur Zutrittskontrolle für bestimmte Bereiche ein. Eine Schulkantine bietet den Schülern das „Bezahlen per Fingerabdruck" an.
2	Verarbeitung von genetischen Daten im Sinne von Artikel 4 Nr. 13 DSGVO, , wenn mindestens ein weiteres folgendes Kriterium aus WP 248 Rev. 01 zutrifft: ▪ Daten zu schutzbedürftigen Betroffenen ▪ Systematische Überwachung ▪ Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen ▪ Bewerten oder Einstufen (Scoring) ▪ Abgleichen oder Zusammenführen von Datensätzen ▪ Automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung ▪ Betroffene werden an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags gehindert	Früherkennung von Erbkrankheiten	Eine Klinik setzt DNA-Tests zur Früherkennung vererblicher Krankheiten bei Neugeborenen ein.
		Genetische Datenbanken zur Abstammungsforschung	Ein Unternehmen bietet einen Dienst an, über den Kunden die eigenen genetischen Daten mit denen Dritter abgleichen können, um mehr über die eigene Abstammung zu erfahren. Dazu pflegt das Unternehmen eine Datenbank mit genetischen Daten einer Vielzahl von Personen.

Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist

Nr.	Maßgebliche Beschreibung der Verarbeitungstätigkeit	Typische Einsatzfelder	Beispiele
3	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 DS-GVO handelt	Träger von großen sozialen Einrichtungen	
		Betrieb eines Insolvenzverzeichnisses	Ein Unternehmen bietet ein umfassendes Verzeichnis über Privatinsolvenzen an.
		Große Anwaltssozietät	Große Rechtsanwaltskanzlei, die im Schwerpunkt familienrechtliche Mandate betreut
4	Umfangreiche Verarbeitung von personenbezogenen Daten über den Aufenthalt von natürlichen Personen	Fahrzeugdatenverarbeitung – Car Sharing / Mobilitätsdienste	Ein Unternehmen bietet einen Car-Sharing-Dienst oder andere Mobilitätsdienstleistungen an und verarbeitet hierfür insbesondere umfangreich Positions- und Abrechnungsdaten.
		Fahrzeugdatenverarbeitung – Zentralisierte Verarbeitung der Messwerte oder Bilderzeugnisse von Umgebungssensoren	Ein Unternehmen erhebt personenbezogene Daten, die Fahrzeuge über ihre Umgebung generieren und ermittelt daraus beispielsweise freie Parkplätze oder verbessert Algorithmen zum automatisierten Fahren.
		Offline-Tracking von Kundenbewegungen in Warenhäusern, Einkaufszentren o. ä.	Ein Unternehmen verarbeitet die GPS-, Bluetooth- und/oder Mobilfunksignale von Passanten und Kunden, um die Laufwege und das Einkaufsverhalten nachverfolgen zu können.
		Verkehrsstromanalyse auf der Grundlage von Standortdaten des öffentlichen Mobilfunknetzes	
5	Zusammenführung von personenbezogenen Daten aus verschiedenen Quellen und Verarbeitung der so zusammengeführten Daten, sofern ▪ die Zusammenführung oder Verarbeitung in großem Umfang vorgenommen werden, ▪ für Zwecke erfolgen, für welche nicht alle der zu verarbeitenden Daten direkt bei den betroffenen Personen erhoben wurden, ▪ die Anwendung von Algorithmen einschließen, die für die betroffenen Personen 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	Fraud-Prevention-Systeme	Zur Prävention von Betrugsfällen verarbeitet der Betreiber eines Online-Shops umfassende Datenmengen. Das Ergebnis der Prüfung ist ein Risikowert, der darüber entscheidet, ob einem Käufer der Rechnungskauf als Zahlungsart angeboten wird oder nicht.
		Scoring durch Auskunfteien, Banken oder Versicherungen	Eine Auskunftei führt ein Scoring im Hinblick auf die Vertrauenswürdigkeit von Personen durch. Eine Bank führt Scoring durch, um das Ausfallrisiko der Rückzahlungen von Personen zu bestimmen. Eine Versicherung führt ein Scoring durch, um das Risiko einer Person im Hinblick auf bestimmte Eigenschaften oder Aktivitäten der Person zur Bestimmung der Höhe einer Versicherungspolice zu bestimmen.

Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist

Nr.	Maßgebliche Beschreibung der Verarbeitungstätigkeit	Typische Einsatzfelder	Beispiele
6	Mobile optisch-elektronische Erfassung personenbezogener Daten in öffentlichen Bereichen, sofern die Daten aus ein oder mehreren Erfassungssystemen in großem Umfang zentral zusammengeführt werden.	Fahrzeugdatenverarbeitung – Umgebungssensoren	Ein Unternehmen erhebt personenbezogene Daten, die Fahrzeuge über ihre Umgebung generieren und ermittelt daraus beispielsweise freie Parkplätze oder verbessert Algorithmen zum automatisierten Fahren.
7	Umfangreiche Erhebung und Veröffentlichung oder Übermittlung von personenbezogenen 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	Betrieb von Bewertungsportalen	Ein Online-Portal bietet Nutzern die Möglichkeit an, Leistungen von Selbstständigen öffentlich feingranular zu bewerten. Online-Bewertungsportal bspw. für Ärzte, Selbstständige oder Lehrer.
		Inkassodienstleistungen – Forderungsmanagement	Ein Unternehmen verarbeitet für seine Kunden in großem Umfang personenbezogene Daten von Schuldnern, insbesondere Vertragsdaten, Rechnungsdaten und Daten über Vermögensverhältnisse von Schuldnern zur Geltendmachung von Forderungen. Ggf. werden Daten an Auskunfteien übermittelt.
		Inkassodienstleistungen – Factoring	Ein Unternehmen lässt sich in großem Umfang Forderungen übertragen um diese auf eigenes Risiko geltend zu machen. Es verbarbeitet hierfür insbesondere Vertragsdaten, Rechnungsdaten, Scoringdaten und Informationen über Vermögensverhältnisse von Schuldnern. Ggf. werden Daten an Auskunfteien übermittelt.
8	Umfangreiche Verarbeitung von personenbezogenen Daten über das Verhalten von Beschäftigten, die zur Bewertung ihrer Arbeitstätigkeit derart eingesetzt werden können, dass sich Rechtsfolgen für die Betroffenen ergeben oder diese Betroffenen in anderer Weise erheblich beeinträchtigt werden	Einsatz von Data-Loss-Prevention Systemen, die systematische Profile der Mitarbeiter erzeugen	Zentrale Aufzeichnung der Aktivitäten (z.B. Internetverkehr, Mailverkehr und die Nutzung von Wechselmedien) am Arbeitsplatz mit dem Ziel, von Seiten des Verantwortlichen unerwünschtes Verhalten (z.B. Versand interner Dokumente) zu erkennen.
		Geolokalisierung von Beschäftigten	Ein Unternehmen lässt Bewegungsprofile von Beschäftigen erstellen (per RFID, Handy-Ortung oder GPS) zur Sicherung des Personals (Wachpersonal, Feuerwehrleute), zum Schutz von wertvollem Eigentum des Arbeitgebers oder eines Dritten (LKW mit Ladung, Geldtransport) oder zur Koordination von Arbeitseinsätzen im Außendienst.
9	Erstellung umfassender Profile über die Interessen, das Netz persönlicher Beziehungen oder die Persönlichkeit der Betroffenen	Betrieb von Dating- und Kontaktportalen	Ein Webportal erstellt Profile der Nutzer um möglichst passende Kontaktvorschläge zu generieren.
		Betrieb von großen Sozialen Netzwerken	

Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist

Nr.	Maßgebliche Beschreibung der Verarbeitungstätigkeit	Typische Einsatzfelder	Beispiele
10	Zusammenführung von personenbezogenen Daten aus verschiedenen Quellen und der Verarbeitung der so zusammengeführten Daten, sofern ▪ die Zusammenführung oder Verarbeitung in großem Umfang vorgenommen werden, ▪ für Zwecke erfolgen, für welche nicht alle der zu verarbeitenden Daten direkt bei den betroffenen Personen erhoben wurden, ▪ die Anwendung von Algorithmen einschließen, die für die betroffenen Personen nicht nachvollziehbar sind, und ▪ der Entdeckung vorher unbekannter Zusammenhänge zwischen den Daten für nicht im Vorhinein bestimmte Zwecke dienen	Big-Data-Analyse von Kundendaten, die mit Angaben aus Drittquellen angereichert wurden	Eine Unternehmen mit umfangreichem Stamm an natürlichen Personen als Kunden, analysiert Daten über das Kaufverhalten der Kunden und die Nutzung der eigenen Webangebote einschließlich des eigenen Webshops, verknüpft mit Bonitätsdaten von dritter Seite und Daten aus der Werbeansprache über soziale Medien einschließlich der vom Betreiber des sozialen Medium bereitgestellten Daten über die angesprochenen Mitglieder, um Informationen zu gewinnen, die zur Steigerung des Umsatzes eingesetzt werden können.
11	Einsatz von künstlicher Intelligenz zur Verarbeitung personenbezogener Daten zur Steuerung der Interaktion mit den Betroffenen oder zur Bewertung persönlicher Aspekte der betroffenen Person	Kundensupport mittels künstlicher Intelligenz	Ein Callcenter wertet automatisiert die Stimmungslage der Anrufer aus. Ein Unternehmen setzt ein System ein, welches mit Kunden durch Konversation interagiert und für deren Beratung personenbezogene Daten durch eine künstliche Intelligenz verarbeitet werden
12	Nicht bestimmungsgemäße Nutzung von Sensoren eines Mobilfunkgeräts im Besitz der betroffenen Personen oder von Funksignalen, die von solchen Geräten versandt werden, zur Bestimmung des Aufenthaltsorts oder der Bewegung von Personen über einen substantiellen Zeitraum	Offline-Tracking von Kundenbewegungen in Warenhäusern, Einkaufszentren o. ä.	Ein Unternehmen verarbeitet die WLAN-, Bluetooth- oder Mobilfunksignale von Passanten und Kunden, um die Laufwege und das Einkaufsverhalten nachverfolgen zu können.
		Verkehrsstromanalyse auf der Grundlage von Standortdaten des öffentlichen Mobilfunknetzes	
13	Automatisierte Auswertung von Video- oder Audio-Aufnahmen zur Bewertung der Persönlichkeit der Betroffenen	Telefongespräch-Auswertung mittels Algorithmen	Ein Callcenter wertet automatisiert die Stimmungslage der Anrufer aus.
14	Erstellung umfassender Profile über die Bewegung und das Kaufverhalten von Betroffenen	Erfassung des Kaufverhaltens unterschiedlicher Personenkreise zur Profilbildung und Kundenbindung unter Zuhilfenahme von Preisen, Preisnachlässen und Rabatten.	Ein Unternehmen verwendet Kundenkarten, welche das Einkaufsverhalten der Kunden erfassen. Als Anreiz zur Verwendung der Kundenkarte erhält der Kunde mit jedem Einkauf Treuepunkte. Mithilfe der gewonnenen Daten erstellt der Anbieter umfassende Kundenprofile.
15	Anonymisierung von besonderen personenbezogenen Daten nach Artikel 9 DS-GVO nicht nur in Einzelfällen (in Bezug auf die Zahl der betroffenen Personen und die Angaben je betroffener Person) zum Zweck der Übermittlung an Dritte	Anonymisierung von besonderen Arten personenbezogener Daten nach Artikel 9	Umfangreiche besondere personenbezogene Daten werden durch ein Apothekenrechenzentrum oder eine Versicherung anonymisiert und zu anderen Zwecken selbst verarbeitet oder an Dritte weitergegeben.

Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist			
Nr.	**Maßgebliche Beschreibung der Verarbeitungstätigkeit**	**Typische Einsatzfelder**	**Beispiele**
16	Verarbeitung von personenbezogenen Daten gemäß Art. 9 Abs. 1 und Art. 10 DS-GVO - auch wenn sie nicht als „umfangreich" im Sinne des Art 35 Abs. 3 lit. b) anzusehen ist - sofern eine nicht einmalige Datenerhebung mittels der innovativen Nutzung von Sensoren oder mobilen Anwendungen stattfindet und diese Daten von einer zentralen Stelle empfangen und aufbereitet werden.	Einsatz von Telemedizin-Lösungen zur detaillierten Bearbeitung von Krankheitsdaten	Ein Arzt nutzt ein Webportal oder setzt eine App an, um mit Patienten mittels Videotelefonie zu kommunizieren und Gesundheitsdaten durch Sensoren beim Patienten (z.B. Blutzucker, Sauerstoffmaske,…) detailliert und systematisch zu erheben und zu verarbeiten.
17	Verarbeitung von Daten gemäß Art. 9 Abs. 1 und Art. 10 DS-GVO - auch wenn sie nicht als „umfangreich" im Sinne des Art 35 Abs. 3 lit. b) anzusehen ist – sofern die Daten durch die Anbieter neuer Technologien dazu verwendet werden, die Leistungsfähigkeit der Personen zu bestimmen.	Zentrale Speicherung der Messdaten von Sensoren, die in Fitnessarmbändern oder Smartphones verbaut sind	Ein Unternehmen bietet einen Dienst an, mit dem Daten aus Fitnessarmbändern zur Verbesserung des Trainings verarbeitet werden.

D Andere hochriskante Verarbeitungstätigkeiten

Diese Liste ist nicht abschließend, sondern ergänzt die in den Absätzen 1 und 3 des Artikels 35 DS-GVO enthaltenen allgemeinen Regelungen. Allgemein gilt, dass für jede Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, die aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, vorab eine Datenschutz-Folgenabschätzung durchgeführt werden muss, insbesondere in den in Absatz 3 genannten Fällen.

Wird die Verarbeitungstätigkeit eines Verantwortlichen in der vorliegenden Liste nicht aufgeführt, so ist daher hieraus nicht der Schluss zu ziehen, dass keine DSFA durchzuführen wäre. Stattdessen ist es Aufgabe des Verantwortlichen, im Wege einer Vorabprüfung einzuschätzen, ob einer der in Art. 35 Abs. 3 DS-GVO genannten Fälle vorliegt oder die Verarbeitung anderweitig 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.

Diese Liste orientiert sich an der allgemeinen, im Arbeitspapier 248 Rev. 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"* beschriebenen Vorgehensweise. Sie ergänzt und konkretisiert diese allgemeine Vorgehensweise.

Der Leitlinie sind folgende neun maßgebliche Kriterien zur Einordnung von Verarbeitungsvorgängen zu entnehmen:

1. **Bewerten oder Einstufen** (Scoring)
2. **Automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung**
3. **Systematische Überwachung**

4. **Vertrauliche oder höchst persönliche Daten**
5. **Datenverarbeitung in großem Umfang**
6. **Abgleichen oder Zusammenführen von Datensätzen**
7. **Daten zu schutzbedürftigen Betroffenen**
8. **Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen**
9. **Betroffene werden an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags gehindert**

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. Im Weiteren wird zum Begriff des Risikos auf das Kurzpapier Nr. 18 „Risiken für die Rechte und Freiheiten natürlicher Personen" der DSK verwiesen.

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.