

Liste von Verarbeitungsvorgängen nach Artikel 35 Absatz 4 Datenschutzgrundverordnung

für die gemäß Artikel 35 Absatz 1 Datenschutzgrundverordnung eine
Datenschutz-Folgenabschätzung von Verantwortlichen im nicht-öffentlichen Bereich
durchzuführen ist

Die Landesbeauftragte für Datenschutz und Informationsfreiheit
Arndtstr. 1
27570 Bremerhaven
Tel.: 0421/361-18332
Fax: 0421/496-18495
E-Mail: office@datenschutz.bremen.de
Internet: www.datenschutz.bremen.de
www.informationsfreiheit.bremen.de

Version 1.1 vom 17.10.2018, ersetzt die Liste vom 18.07.2018

A Gesetzliche Grundlage

Die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates (EU-Datenschutzgrundverordnung – DSGVO) regelt im Abschnitt 3 „Datenschutz-Folgenabschätzung und vorherige Konsultation“ des Kapitels IV „Verantwortlicher und Auftragsverarbeiter“ die Rahmenbedingungen zur sogenannten Datenschutz-Folgenabschätzung (kurz: DSFA; im Englischen Data Protection Impact Assessment oder DPIA). Artikel 35 DSGVO nennt dabei die Grundsätze, bei welchen Fällen eine DSFA durchzuführen ist und was diese enthält. Artikel 36 DSGVO 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 Artikel 35 Absatz 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 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 Artikel 64 Absatz 3 Datenschutzgrundverordnung abgegebenen Stellungnahme des Europäischen Datenschutzausschusses 05/2018 vom 25.09.2018.

Führt ein Verantwortlicher Verarbeitungsvorgänge aus, die in Artikel 35 Absatz 3 DSGVO oder der vorliegenden Liste aufgeführt sind, ohne vorab eine DSFA durchgeführt zu haben, so kann die zuständige Aufsichtsbehörde wegen Verstoßes gegen Artikel 35 Absatz 1 DSGVO von ihren Abhilfebefugnissen gemäß Artikel 58 Absatz 2 DSGVO einschließlich der Verhängung von Geldbußen gemäß Artikel 83 Absatz 4 DSGVO Gebrauch machen. Gegen einen derartigen Beschluss der Aufsichtsbehörde steht der Rechtsweg gemäß Artikel 78 DSGVO offen.

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

Das Dokument hat nicht den Anspruch der Vollständigkeit, wenngleich versucht wird, möglichst viele der DSFA-pflichtigen Verarbeitungsvorgänge zu berücksichtigen. Auf Grund der Schnelllebigkeit 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. Die DSK wird hierfür einen Prozess erarbeiten, wie Verarbeitungstätigkeiten für die Muss-Liste vorschlagen, beurteilt und aufgenommen werden. Änderungen an Einträgen der Muss-Liste werden dokumentiert, so dass die Muss-Liste eine entsprechende Versionshistorie erhalten wird.

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 Artikel 35 Absatz 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“ (WP 248 Rev. 01 der Artikel-29-Datenschutzgruppe und das Kurzpapier Nr. 18 „Risiken für die Rechte und Freiheiten natürlicher Personen“ der DSK verwiesen.

C Liste nach Artikel 35 Absatz 4 DSGVO

Maßgebliche Kriterien zur Einordnung von Verarbeitungsvorgängen sind in der Leitlinie in WP 248 der Artikel-29-Datenschutzgruppe 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.

Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist

Nr.	Maßgebliche Beschreibung der Verarbeitungstätigkeit	Typische Einsatzfelder	Beispiele
1	<p>Verarbeitung von biometrischen Daten zur eindeutigen Identifizierung natürlicher Personen, wenn mindestens ein weiteres folgendes Kriterium aus WP 248 Rev. 01 zutrifft:</p> <ul style="list-style-type: none"> • 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 	<p>Verwendung von biometrischen Systemen zur Zutrittskontrolle oder für Abrechnungszwecke.</p>	<p>Ein Unternehmen setzt flächendeckend Fingerabdrucksensoren zur Zutrittskontrolle für bestimmte Bereiche ein.</p> <p>Eine Schulkantine bietet den Schülern das „Bezahlen per Fingerabdruck“ an.</p>
2	<p>Verarbeitung von genetischen Daten im Sinne von Artikel 4 Nr. 13 DSGVO, wenn mindestens ein weiteres folgendes Kriterium aus WP 248 Rev. 01 zutrifft:</p> <ul style="list-style-type: none"> • 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. 	<p>Früherkennung von Erbkrankheiten</p> <p>Genetische Datenbanken zur Abstammungsforschung</p>	<p>Eine Klinik setzt DNA-Tests zur Früherkennung vererblicher Krankheiten bei Neugeborenen ein.</p> <p>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.</p>
3	<p>Umfangreiche Verarbeitung von Daten, die dem Sozial-, einem Berufs- oder besonderen Amtsgeheimnis unterliegen, auch wenn es sich nicht um Daten gemäß Artikel 9 Absatz 1 und 10 DSGVO handelt</p>	<p>Träger von großen sozialen Einrichtungen</p> <p>Betrieb eines Insolvenzverzeichnisses</p> <p>Große Anwaltssozietät</p>	<p>Ein Unternehmen bietet ein umfassendes Verzeichnis über Privatinsolvenzen an.</p> <p>Große Rechtsanwaltskanzlei, die im Schwerpunkt familienrechtliche Mandate betreut.</p>

4	<p>Umfangreiche Verarbeitung von personenbezogenen Daten über den Aufenthalt von natürlichen Personen.</p>	<p>Fahrzeugdatenverarbeitung – Car Sharing / Mobilitätsdienste</p> <p>Fahrzeugdatenverarbeitung – Zentralisierte Verarbeitung der Messwerte oder Bilderzeugnisse von Umgebungssensoren</p> <p>Offline-Tracking von Kundenbewegungen in Warenhäusern, Einkaufszentren oder ähnliches</p> <p>Verkehrsstromanalyse auf der Grundlage von Standortdaten des öffentlichen Mobilfunknetzes</p>	<p>Ein Unternehmen bietet einen Car-Sharing-Dienst oder andere Mobilitätsdienstleistungen an und verarbeitet hierfür insbesondere umfangreich Positions- und Abrechnungsdaten.</p> <p>Ein Unternehmen erhebt personenbezogene Daten, die Fahrzeuge über ihre Umgebung generieren und ermittelt daraus beispielsweise freie Parkplätze oder verbessert Algorithmen zum automatisierten Fahren.</p> <p>Ein Unternehmen verarbeitet die GPS-, Bluetooth- und/oder Mobilfunksignale von Passanten und Kunden, um die Laufwege und das Einkaufsverhalten nachverfolgen zu können.</p>
5	<p>Zusammenführung von personenbezogenen Daten aus verschiedenen Quellen und Verarbeitung der so zusammengeführten Daten, sofern</p> <ul style="list-style-type: none"> • 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. 	<p>Fraud-Prevention-Systeme</p> <p>Scoring durch Auskunfteien, Banken oder Versicherungen</p>	<p>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.</p> <p>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.</p>
6	<p>Mobile optisch-elektronische Erfassung personenbezogener Daten in öffentlichen Bereichen, sofern die Daten aus ein oder mehreren Erfassungssystemen in großem Umfang zentral zusammengeführt werden.</p>	<p>Fahrzeugdatenverarbeitung – Umgebungssensoren</p>	<p>Ein Unternehmen erhebt personenbezogene Daten, die Fahrzeuge über ihre Umgebung generieren und ermittelt daraus beispielsweise freie Parkplätze oder verbessert Algorithmen zum automatisierten Fahren.</p>
7	<p>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</p>	<p>Betrieb von Bewertungsportalen</p> <p>Inkassodienstleistungen – Forderungsmanagement</p> <p>Inkassodienstleistungen – Factoring</p>	<p>Ein Online-Portal bietet Nutzern die Möglichkeit an, Leistungen von Selbstständigen öffentlich feingranular zu bewerten. Online-Bewertungsportal beispielsweise für Ärzte, Selbstständige oder Lehrer.</p> <p>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. Gegebenenfalls werden Daten an Auskunfteien übermittelt.</p> <p>Ein Unternehmen lässt sich in großem Umfang Forderungen übertragen um diese auf eigenes Risiko geltend zu</p>

			machen. Es verarbeitet hierfür insbesondere Vertragsdaten, Rechnungsdaten, Scoringdaten und Informationen über Vermögensverhältnisse von Schuldern. Gegebenenfalls, werden Daten an Auskunftfeien 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 Geolokalisierung von Beschäftigten	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. Ein Unternehmen lässt Bewegungsprofile von Beschäftigten 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 Betrieb von großen Sozialen Netzwerken	Ein Webportal erstellt Profile der Nutzer um möglichst passende Kontaktvorschläge zu generieren.
10	Zusammenführung von personenbezogenen Daten aus verschiedenen Quellen und der Verarbeitung der so zusammengeführten Daten, sofern <ul style="list-style-type: none"> • 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	Ein 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 Werbeanzeige 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 oder ähnliches. Verkehrsstromanalyse auf der Grundlage von Standortdaten des öffentlichen Mobilfunknetzes	Ein Unternehmen verarbeitet die WLAN-, Bluetooth- oder Mobilfunksignale von Passanten und Kunden, um die Laufwege und das Einkaufsverhalten nachverfolgen zu können.
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 DSGVO 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.
16	Verarbeitung von personenbezogenen Daten gemäß Artikel 9 Absatz 1 und Artikel 10 DSGVO - auch wenn sie nicht als „umfangreich“ im Sinne des Artikel 35 Absatz 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 Artikel 9 Absatz 1 und Artikel 10 DSGVO - auch wenn sie nicht als „umfangreich“ im Sinne des Artikel 35 Absatz 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.