Liste von Verarbeitungsvorgängen nach Art. 35 Abs. 4 DSGVO

Entwurf zur Vorlage beim Europäischen Datenschutzausschuss nach Art. 35 Abs. 6 DSGVO

Ab dem 25. Mai 2018 ist die Datenschutz-Grundverordnung (DSGVO) in allen Mitgliedstaaten der Europäischen Union und somit auch in Deutschland als unmittelbar geltendes Recht anzuwenden. Zu den Pflichten des Verantwortlichen gehört es, bei Formen der Verarbeitung, die ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge haben, eine Datenschutz-Folgenabschätzung (DSFA) nach Art. 35 DSGVO durchzuführen.

Die Durchführung der Datenschutz-Folgenabschätzung dient dazu, in einem systematischen Vorgehen geplante Verarbeitungsvorgänge zu beschreiben, ihre Notwendigkeit und Verhältnismäßigkeit zu beurteilen, die Risiken für die Rechte und Freiheiten der betroffenen Personen zu bewerten und zur Bewältigung dieser Risiken vorab Abhilfemaßnahmen festzulegen.

Hilfestellungen für die Durchführung einer DSFA

Die Konferenz der Datenschutzbehörden des Bundes und der Länder hat im Rahmen ihrer Kurzpapiere zur Umsetzung der DSGVO auch die Kurzpapiere Nr. 5 zur Datenschutz-Folgenabschätzung und Nr. 18 zum Risikobegriff veröffentlicht. Die beiden Kurzpapiere sind neben weiteren Kurzpapieren unter https://www.lfd.niedersachsen.de/startseite/dsgvo/anwendung_dsgvo_kurzpapiere abrufbar. Auch die Art.-29-Gruppe, ein unabhängiges europäisches Beratungsgremium für den Schutz personenbezogener Daten und die Privatsphäre, hat eine Leitlinie zur Datenschutz-Folgenabschätzung und dem Risikobegriff erstellt. Sie kann unter https://www.lfd.niedersachsen.de/startseite/dsgvo/leitlinien_art_29gruppe/ abgerufen werden.

Grundlage für die vorliegende Liste

Nach Art. 35 Abs. 4 DSGVO erstellt die Aufsichtsbehörde eine Liste von Verarbeitungsvorgängen, für die aufgrund eines voraussichtlich hohen Risikos für die Rechte und Freiheiten natürlicher Personen eine Datenschutz-Folgenabschätzung durchzuführen ist. Die Landesbeauftragte für den Datenschutz Niedersachsen macht von dieser Norm mit der vorliegenden Liste im Rahmen ihrer Zuständigkeit Gebrauch.

Die Einträge beruhen auf der Anwendung der oben genannten Leitlinie der Art.-29-Gruppe. Der Leitlinie sind folgende maßgebliche Kriterien zur Einordnung des Risikos von Verarbeitungsvorgängen zu entnehmen (S. 10 ff.):

a) Vertrauliche oder höchst persönliche Daten

(“Sensitive data or data of a highly personal nature”)

b) Daten zu schutzbedürftigen Betroffenen
(“Data concerning vulnerable data subjects”)

c) Datenverarbeitung in großem Umfang
(“Data processed on a large scale”)

d) Systematische Überwachung
(“Systematic monitoring”)

e) Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen
(“Innovative use or applying new technological or organisational solutions“)

f) Bewerten oder Einstufen (Scoring)
(“Evaluation or scoring”)

g) Abgleichen oder Zusammenführen von Datensätzen
(“Matching or combining datasets”)

h) Automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung
(“Automated-decision making with legal or similar significant effect”)

i) 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”)

Sind zwei dieser Kriterien erfüllt, ist ausweislich der Leitlinie in den meisten Fällen eine Datenschutz-Folgenabschätzung durchzuführen. Je mehr Kriterien erfüllt sind, desto wahrscheinlicher ist es, dass eine Datenschutz-Folgenabschätzung durchzuführen ist. Es ist aber auch möglich, dass ein hohes Risiko gegeben ist, wenn nur ein Kriterium erfüllt ist.

Umgang mit der vorliegenden Liste

Ist ein Verarbeitungsvorgang in der Liste aufgeführt, so ist für diesen Verarbeitungsvorgang eine Datenschutz-Folgenabschätzung zu erstellen. Die Liste ist aber nicht abschließend. Wenn ein Verarbeitungsvorgang nicht auf der Liste aufgeführt ist, kann daraus nicht geschlossen werden, dass für diesen Verarbeitungsvorgang keine Datenschutz-Folgenabschätzung durchzuführen ist. Es ist dann zu prüfen, ob einer der Fälle aus Art. 35 Abs. 3 DSGVO vorliegt oder ob ein hohes Risiko nach Art. 35 Abs. 1 DSGVO vorliegt, obwohl der Verarbeitungsvorgang nicht auf der Liste steht und kein Fall aus Art. 35 Abs. 3 DSGVO vorliegt.

Für Verantwortliche, die prüfen, ob für einen Verarbeitungsvorgang eine Datenschutz-Folgenabschätzung durchzuführen ist, ergibt sich damit folgende Prüfungsreihenfolge:

1. Prüfung, ob der Verarbeitungsvorgang auf der vorliegenden Liste genannt ist.
2. Wenn der Verarbeitungsvorgang auf der Liste nicht genannt ist, ist zu prüfen, ob der Verarbeitungsvorgang einen Fall nach Art. 35 Abs. 3 DSGVO darstellt.
3. Handelt es sich bei dem Verarbeitungsvorgang auch nicht um einen Fall des Art. 35 Abs. 3 DSGVO, dann ist zu prüfen, ob dennoch ein hohes Risiko nach Art. 35 Abs. 1

DSGVO vorliegt. Ist dies nicht der Fall, muss eine Datenschutz-Folgenabschätzung nicht durchgeführt werden.

Nach Art. 6 Abs. 1 DSGVO ist eine Verarbeitung nur dann rechtmäßig, wenn eine der dort genannten Bedingungen vorliegt. Mit der vorliegenden Liste wird keine Aussage darüber getroffen, ob für einen Verarbeitungsvorgang eine Rechtsgrundlage vorliegt oder nicht. Ein Eintrag auf der Liste bedeutet daher weder, dass eine Verarbeitung verboten ist, noch dass ein Verarbeitungsvorgang allein auf der Grundlage einer Datenschutz-Folgenabschätzung durchgeführt werden kann.

Die Liste macht es an mehreren Stellen zur Voraussetzung einer hochriskanten Verarbeitung, dass es sich um eine „umfangreiche Verarbeitung“ handelt. Die DSGVO definiert den Begriff nicht, sondern gibt nur in Erwägungsgrund 91 einige Anhaltspunkte. Es ist derzeit nicht möglich, hier konkrete Zahlen festzulegen. Die Art.-29-Gruppe hat jedoch in der oben genannten Leitlinie und in ihrer Leitlinie in Bezug auf Datenschutzbeauftragte Stellung dazu genommen, welche Aspekte bei der Bestimmung einer „umfangreichen Verarbeitung“ zu berücksichtigen sind und nennt Beispiele, die den Verantwortlichen bei der Prüfung helfen.

In der ersten Spalte erfolgt zur einfachen Bezugnahme eine Nummerierung. In der zweiten Spalte findet sich die maßgebliche Beschreibung des Verarbeitungsvorgangs. Fällt ein Verarbeitungsvorgang unter diese Beschreibung, dann ist für ihn eine Datenschutz-Folgenabschätzung durchzuführen. Lässt sich ein Verarbeitungsvorgang nicht unter die zweite Spalte subsumieren, ist nach dem oben dargestellten Schema weiter zu prüfen. Die dritte und die vierte Spalte enthalten zur Veranschaulichung typische Einsatzfelder und Beispiele für Verarbeitungsvorgänge, die unter die zweite Spalte zu subsumieren wären. In der Liste für den öffentlichen Bereich konnte auf die dritte und vierte Spalte verzichtet werden.

Führt ein Verantwortlicher hochriskante Verarbeitungsvorgänge aus, ohne vorab eine Datenschutz-Folgenabschätzung 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 einschließlich der Verhängung von Geldbußen gemäß Art. 83 Abs. 4 DSGVO Gebrauch machen. Gegen einen derartigen Beschluss der Aufsichtsbehörde steht der Rechtsweg gemäß Art. 78 DSGVO offen.

Liste von Verarbeitungsvorgängen nach Art. 35 Abs. 4 DSGVO für den öffentlichen und den nichtöffentlichen Bereich

Nr.	Maßgebliche Beschreibung des Verarbeitungsvorgangs	Typische Einsatzfelder	Beispiele
1	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 Art. 10 DSGVO handelt	• Sozialleistungsträger • Große Anwaltssozietäten	Eine große Rechtsanwaltskanzlei, die schwerpunktmäßig familienrechtliche Mandate betreut.
2	Umfangreiche Verarbeitung von personenbezogenen Daten über den Aufenthalt von natürlichen Personen	• Fahrzeugdatenverarbeitung - Car Sharing/Mobilitätsdienste • Fahrzeugdatenverarbeitung – Zentralisierte Verarbeitung der Messwerte oder Bilderzeugnisse von Umgebungssensoren • Offline-Tracking von Kundenbewegungen in Warenhäusern, Einkaufszentren o. ä. • Verkehrsstromanalyse auf der Grundlage von Standortdaten des öffentlichen Mobilfunknetzes	Ein Unternehmen bietet einen Car-Sharing-Dienst oder andere Mobilitätsdienstleistungen an und verarbeitet hierfür insbesondere umfangreich Positions- und Abrechnungsdaten. Ein Unternehmen erhebt personenbezogene Daten, die Fahrzeuge über ihre Umgebung generieren und ermittelt daraus beispielsweise freie Parkplätze oder verbessert Algorithmen zum automatisierten Fahren. Ein Unternehmen verarbeitet die WLAN-, Bluetooth- oder Mobilfunksignale von Passanten und Kunden, um die Laufwege und das Einkaufsverhalten nachverfolgen zu können.
3	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 Personenerhoben wurden,	• Fraud-Prevention-Systeme • Scoring durch Auskunfteien, Banken oder Versicherungen	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.

	• 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		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.
4	Mobile optisch-elektronische Erfassung personenbezogener Daten in öffentlichen Bereichen, sofern die Daten aus verschiedenen 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.
5	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 • Inkassodienstleistungen – Forderungsmanagement • Inkassodienstleistungen – Factoring	Ein Online-Portal bietet Nutzern die Möglichkeit an, Leistungen von Selbstständigen öffentlich feingranular zu bewerten. Z.B. ein Online-Bewertungsportal für Ärzte, Selbstständige oder Lehrer. 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. Ein Unternehmen lässt sich in großem Umfang Forderungen übertragen um diese auf eigenes Risiko geltend zu ma-

			chen. Es verbarbeitet hierfür insbesondere Vertragsdaten, Rechnungsdaten, Scoringdaten und Informationen über Vermögensverhältnisse von Schuldnern. Ggf. werden Daten an Auskunfteien übermittelt.
6	Verarbeitung von umfangreichen personenbezogenen Daten über das Verhalten von Beschäftigten, die zur Bewertung ihrer Arbeitstätigkeit derart eingesetzt werden können, dass sich Rechtsfolgen für die betroffenen Personen ergeben, oder diese in andere Weise erheblich beeinträchtigen	• Einsatz von Data-Loss-Prevention Systemen, die systematische Profile der Mitarbeiter erzeugen • Geolokalisierung von Beschäftigten	Zentrale Aufzeichnung der Aktivitäten am Arbeitsplatz (z.B. Internetverkehr, Mailverkehr und die Nutzung von Wechselmedien) mit dem Ziel, von Seiten des Verantwortlichen unerwünschtes Verhalten (z.B. Versand interner Dokumente) zu erkennen. Ein Unternehmen erstellt Bewegungsprofile von Beschäftigen (z.B. 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.
7	Erstellung umfassender Profile über die Interessen, das Netz persönlicher Beziehungen oder die Persönlichkeit der betroffenen Personen	• Betrieb von Dating- und Kontaktportalen • Betrieb von großen Sozialen Netzwerken	Ein Dating Portal erstellt Profile der Nutzer um möglichst passende Kontaktvorschläge zu generieren.
8	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 Personen erhoben wurden,	• Analyse von Kundendaten, die mit Angaben aus Drittquellen angereichert wurden. • Tätigkeit von Auskunfteien	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

	• die Anwendung von Algorithmen einschließen, die für die betroffenen Personen nicht nachvollziehbar sind		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.
9	Einsatz von künstlicher Intelligenz zur Verarbeitung personenbezogener Daten, zur Steuerung der Interaktion mit den betroffenen Personen oder zur Bewertung persönlicher Aspekte der betroffenen Personen	• Kundensupport mittels künstlicher Intelligenz	Ein Unternehmen setzt ein System ein, welches mit Kunden durch Konversation interagiert und für deren Beratung personenbezogene Daten durch eine künstliche Intelligenz verarbeitet.
10	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. • 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.
11	Automatisierte Auswertung von Video- oder Audio-Aufnahmen zur Bewertung der Persönlichkeit von betroffenen Personen	• Auswertung von Telefongesprächen mittels Algorithmen	Ein Callcenter wertet automatisiert die Stimmungslage der Anrufer aus.
12	Erhebung personenbezogener Daten über Schnittstellen persönlicher elektronischer Geräte, die nicht gegen ein unbefugtes Auslesen geschützt sind, das die betroffenen Personen nicht erkennen können	• 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.
13	Umfangreiche Anonymisierung von besonderen Kategorien personenbezogener Daten nach Artikel 9 DS-GVO, falls diese (ggf. vermeintlich) anonymen Daten an Dritte weitergegeben oder zu nicht nur internen statistischen Zwecken verarbeitet werden sollen	• Forschung mit medizinischen Daten	Umfangreiche besondere personenbezogene Daten werden durch ein Apothekenrechenzentrum oder eine Versiche-

			rung anonymisiert und zu anderen Zwecken selbst verarbeitet oder an Dritte weitergegeben.
14	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 eine innovative Nutzung von digitalen Fernkommunikationsmitteln erfolgt.	• Einsatz von Telemedizin-Lösungen zur detaillierten Bearbeitung von Krankheitsdaten	Ein Hausarzt bietet eine Telefonsprechstunde über ein Webportal oder eine App an.
15.	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 durch die Anbieter neuer Technologien dazu verwendet werden, die Leistungsfähigkeit der Betroffenen 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.

Liste von Verarbeitungsvorgängen nach Art. 35 Abs. 4 DSGVO ausschließlich für den öffentlichen Bereich

Nr.	Maßgebliche Beschreibung des Verarbeitungsvorgangs
1	Umfangreiche Erhebung und Verarbeitung von personenbezogenen Daten im Rahmen der Kinder- und Jugendhilfe insbesondere der Beratung und Beantragung von Hilfen zur Erziehung, Eingliederungshilfe für seelisch behinderte Kinder und Jugendliche und Unterstützung bei der Ausübung der Personensorge und des Umgangsrechts, Förderung von Kindern in Kindertagesbetreuung, Hilfe für Junge Volljährig sowie bei der Beratung und Unterstützung bei der Ausübung der Personensorge und des Umgangsrechts (Verarbeitungstätigkeiten der Kinder-und Jugendhilfe)
2	Umfangreiche Erhebung von Verarbeitung von personenbezogenen Daten für die Aufgaben der Jobcenter insbesondere die Leistungsgewährung zur Sicherung des Lebensunterhalts, Leistungen der Unterkunft und Heizung. Leistungsrecht und die Vermittlung in Arbeit inkl. Eingliederungsleistungen und auch kommunale Leistungen wie Suchtberatung oder Schuldnerberatung.
3	Verarbeitung der Meldedaten, Melderegister und Spiegelregister von Kommunen und bei landesweiten Verfahren.
4	Verfahren zur Führung von Personenstandsregistern von Kommunen und bei landesweiten Verfahren.
5	Verarbeitung von Personalausweis- und Passanträgen sowie der jeweiligen Register bei Kommunen und bei landesweiten Verfahren.
6	Umfangreiche Erhebung und Verarbeitung von personenbezogenen Daten im Zuge der Beantragung von Sozialhilfe, insbesondere als Grundsicherung im Alter oder bei voller Erwerbsminderung und bei Hilfen zur Gesundheit, bei Eingliederungshilfen für behinderte Menschen, Hilfe zur Pflege, Hilfe zur

	Überwindung besonderer sozialer Schwierigkeiten und die Hilfe in anderen Lebenslagen (Verarbeitungstätigkeiten der Sozialhilfe).
7	Umfangreiche Verarbeitung personenbezogener Daten im Rahmen der amtlichen Statistik, deren Erhebung, Speicherung und Verarbeitung, insbesondere der Anonymisierungsprozesse sowie deren Anonymisierung und statistische Aufbereitung vor/für die Übermittlung der Informationen an Dritte (Verarbeitung der personenbezogenen Daten im Rahmen der amtlichen Statistik).
8	Verarbeitung von personenbezogenen Schülerdaten durch Lernplattformen, bei denen die Verarbeitung durch einen zentralen Auftragsverarbeiter erfolgt.

Die Landesbeauftragte für den Datenschutz Niedersachsen
Prinzenstr. 5, 30159 Hannover
Tel.: 0511 - 120 4500 / Fax: 0511 - 120 4599
eMail: poststelle@lfd.niedersachsen.de

Stand: 25. Mai 2018