Der Landesbeauftragte für den
DATENSCHUTZ und die
INFORMATIONSFREIHEIT
Rheinland-Pfalz

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

VORVERSION

Vorversion
Stand: 24.05.2018

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 (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 nicht-öffentlichen Bereich, darunter auch solche, die mit dem Angebot von Waren und Dienstleistungen für betroffene Personen in mehreren Mitgliedsstaaten verbunden sind. Sie unterliegt daher aufgrund von Art. 35 Abs. 6 DS-GVO dem Kohärenzverfahren gemäß Art. 63 DS-GVO. Dieses konnte aufgrund des sich erst noch bildenden Datenschutz-Ausschusses bisher noch nicht durchgeführt werden. Aufgrund des noch durchzuführenden Kohärenzverfahrens handelt es sich bei dieser Liste um eine Vorversion.

Führt ein Verantwortlicher Verarbeitungsvorgänge aus, die in Art. 35 Abs. 3 DS-GVO oder der vorliegenden Liste aufgeführt sind, ohne vorab eine DSFA durchgeführt zu haben, 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.

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 und nach Art. 35 Abs. 6 DS-GVO im Kohärenzverfahren gemäß Art. 63 DS-GVO behandelt werden kann, sofern die Bedingungen hierzu erfüllt sind. 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 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.

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.

Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist			
Nr.	Maßgebliche Beschreibung der Verarbeitungstätigkeit	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 10 DS-GVO handelt	Betrieb eines Insolvenzverzeichnisses Sozialleistungsträger Große Anwaltssozietät	Ein Unternehmen bietet ein umfassendes Verzeichnis über Privatinsolvenzen an.
2	Umfangreiche Verarbeitung von Daten über den Aufenthalt von 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 Daten, die Fahrzeuge über ihre Umgebung generieren und ermittelt daraus beispielsweise freie Parkplätze oder verbessert Algorithmen zum automatisierten Fahren. Ein Unternehmen verarbeitet die GPS- und WLAN-Daten 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 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	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. 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	Verarbeitung von Daten gemäß Art. 9 Abs. 1 und 10 DS-GVO durch Auftragsverarbeiter, denen von einem Gericht oder einer Verwaltungsbehörde eines Drittlands die Pflicht auferlegt werden kann, diese Daten entgegen Art. 48 DS-GVO zu exportieren oder offenzulegen	Einsatz von Dienstleistern mit Sitz außerhalb der EU durch pädagogische Einrichtungen Einsatz von Dienstleistern mit Sitz außerhalb der EU durch medizinische Leistungserbringer	Datenverarbeitung von personenbezogenen Schülerdaten gemäß Art. 9 Abs. 1 DS-GVO in einer öffentlichen Cloud (z.B. in einem digitalen Klassenbuch – Dokumentation von Fehlzeiten, Entschuldigungen oder andere Dokumentationen

5	Mobile und für die Betroffenen intransparente optoelektronische Erfassung öffentlicher Bereiche	Fahrzeugdatenverarbeitung – Umgebungssensoren	Ein Unternehmen erhebt Daten, die Fahrzeuge über ihre Umgebung generieren und ermittelt daraus beispielsweise freie Parkplätze oder verbessert Algorithmen zum automatisierten Fahren.
6	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	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.
7	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	Einsatz von Data-Loss-Prevention Systemen, die systematische Profile der Mitarbeiter erzeugen	Zentrale Aufzeichnung des Internetverlaufs und der Aktivitäten 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.
8	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	
9	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,	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

	• 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		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.
10	Einsatz von künstlicher Intelligenz zur Verarbeitung personenbezogener Daten zur Steuerung der Interaktion mit den Betroffenen oder zur Bewertung persönlicher Aspekte der Betroffenen	Telefongespräch-Auswertung mittels Algorithmen	Ein Callcenter wertet automatisiert die Stimmungslage der Anrufer aus.
11	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	Offline-Tracking von Kundenbewegungen in Warenhäusern, Einkaufszentren o. ä. Verkehrsstromanalyse auf der Grundlage von Standortdaten des öffentlichen Mobilfunknetzes	Ein Unternehmen verarbeitet die GPS- und WLAN-Daten von Passanten und Kunden, um die Laufwege und das Einkaufsverhalten nachverfolgen zu können.
12	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.
13	Erhebung personenbezogener Daten über Schnittstellen persönlicher elektronischer Geräte, die nicht gegen ein unbefugtes Auslesen geschützt sind, das die Betroffenen nicht erkennen können	Einsatz von RFID/NFC durch Apps oder Karten	Eine Bank setzt die NFC-Technologie bei Geldkarten ein, um den Zahlungsverkehr zu erleichtern.
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	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 eine nicht einmalige Datenerhebung mittels 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 bietet eine App an, um Patienten detailliert und systematisch zu behandeln.
16	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 mittels Sensoren erhoben, an einer zentralen Stelle verarbeitet und dazu verwendet werden, die Leistungsfähigkeit des Betroffenen zu bestimmen	Zentrale Speicherung der Messdaten von Sensoren, die in Fitnessarmbändern oder Smartphones verbaut sind	