Vorläufige Liste von Verarbeitungsvorgängen nach Art. 35 Abs. 4 DS-GVO

für die gemäß Art. 35 Abs. 1 DS-GVO eine Datenschutz-Folgenabschätzung von Verantwortlichen durchzuführen ist

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 Auftragverarbeiter" 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 bei öffentlichen und bei nichtöffentlichen Stellen (Verantwortlichen nach Art, 4 Nr. 7 DS-GVO) 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 auch Verarbeitungsvorgänge die mit dem Angebot von Waren und Dienstleistungen für betroffene Personen in mehreren Mitgliedstaaten verbunden sind. Sie unterliegt daher aufgrund von Art. 35 Abs. 6 DS-GVO dem Kohärenzverfahren gemäß Art. 63 DS-GVO.

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-DSFA**" bezeichnet – gängige Begriffe in anderen Ländern sind hierfür auch „Blacklist" und „Positivliste".

B Ziel dieses Dokuments

Weil es derzeit nur eine von der Datenschutzkonferenz am 06.06.2018 verabschiedete gemeinsame Liste aller Aufsichtsbehörden in Deutschland für den nichtöffentlichen Bereich gibt, gilt diese Liste bis auf weiteres hinsichtlich des öffentlichen Bereichs nur für Stellen in Thüringen. Auch die Liste für den nicht-öffentlichen Bereich gilt vorläufig, da diese noch nicht vom europäischen Datenschutzausschuss genehmigt worden ist. Sobald die Liste genehmigt ist, gilt sie uneingeschränkt.
Berücksichtigt wurde 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"" (WP 248) der Art. 29 Gruppe der Europäischen Kommission.

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.

Unter Berücksichtigung der speziellen Verarbeitungssituationen ist eine Liste für den **öffentlichen Bereich** vorangestellt. Kumulativ gilt für den öffentlichen Bereich auch die **gemeinsame Liste (öffentlicher und nicht-öffentlicher Bereich**), soweit es nicht europarechtskonforme gesetzliche Ausnahmen gibt.

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 oben genannten Leitlinien, auf das Kurzpapier Nr. 18 „Risiken für die Rechte und Freiheiten natürlicher Personen" und das Kurzpapier Nr. 5 „Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO" der Datenschutzkonferenz (DSK) verwiesen.

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

Wenn eine Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfang, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, ist vorab eine DSFA durchzuführen. Maßgebliche Kriterien zur Einordnung von Verarbeitungsvorgängen, mit denen ein hohes Risiko verbunden sein könnte sind den Leitlinien 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 dieser 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.

Spezielle Liste für den öffentlichen Bereich

Nr.	Maßgebliche Beschreibung der Verarbeitungstätigkeit	Beispiele
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 Volljährige sowie bei der Beratung und Unterstützung bei der Ausübung der Personensorge und des Umgangsrechts (Verarbeitungstätigkeiten der Kinder-und Jugendhilfe)	Eingliederungshilfe für seelisch behinderte Kinder
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. (Kommunales Jobcenter – Fachverfahren zur Verwaltung und Dokumentation der Förderung und Vermittlung von ALG II -Empfängern)	Leistungsgewährung zur Sicherung des Lebensunterhalts im Rahmen von ALG II
3	Verarbeitung der Meldedaten, Melderegister und Spiegelregister von Mittel- und Großstädten sowie vergleichbaren Kommunen und bei landesweiten Verfahren	
4	Verfahren zur Führung von Personenstandsregistern von Mittel- und Großstädten sowie vergleichbarer Kommunen und bei landesweiten Verfahren	
5	Verarbeitung von Personalausweis- und Passanträgen sowie der jeweiligen Register bei Mittel- und Großstädten sowie vergleichbarer 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)	

Gemeinsame 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 Träger von großen sozialen Einrichtungen Große Anwaltssozietät	Ein Unternehmen bietet ein umfassendes Verzeichnis über Privatinsolvenzen an. Große Rechtsanwaltskanzlei, die im Schwerpunkt 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 GPS-, Bluetooth- und/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 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 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	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.

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	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.
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 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.
7	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	
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,	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

	• 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		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.
9	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
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 der Betroffenen	Telefongespräch-Auswertung 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 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.
13	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.
14	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.
15	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	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

	der innovativen Nutzung von Sensoren oder mobilen Anwendungen stattfindet und diese Daten von einer zentralen Stelle empfangen und aufbereitet werden.		durch Sensoren beim Patienten (z.B. Blutzucker, Sauerstoffmaske,...) detailliert und systematisch zu erheben und zu verarbeiten.
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 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.