Der Bayerische Landesbeauftragte
für den Datenschutz

Datenschutz-Folgenabschätzung

Bayerische Blacklist

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

Stand: 1. März 2019

Der Bayerische Landesbeauftragte für den Datenschutz
80538 München | Wagmüllerstraße 18 | Telefon: +49 89 21 26 72-0
E-Mail: poststelle@datenschutz-bayern.de | https://www.datenschutz-bayern.de

Einführung

Nach Art. 35 Abs. 1 Datenschutz-Grundverordnung (DSGVO) hat der Verantwortliche für einen Verarbeitungsvorgang eine **Datenschutz-Folgenabschätzung** durchzuführen, wenn die Form der Verarbeitung „voraussichtlich ein **hohes Risiko** für die Rechte und Freiheiten natürlicher Personen" zur Folge hat.

Die Datenschutz-Grundverordnung selbst nennt in **Art. 35 Abs. 3 DSGVO** konkretisierend drei Arten von Verarbeitungsvorgängen bei denen in jedem Fall eine Datenschutz-Folgenabschätzung (DSFA) erforderlich ist:

- die **systematische und umfassende 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,
- die **umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten** gemäß Art. 9 Abs. 1 DSGVO oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DSGVO und
- die **systematische umfangreiche Überwachung** öffentlich zugänglicher Bereiche.

Art. 35 Abs. 4 DSGVO verpflichtet die Datenschutz-Aufsichtsbehörden zudem, eine **Liste von Verarbeitungsvorgängen** zu erstellen und zu veröffentlichen, für die in jedem Fall eine Datenschutz-Folgenabschätzung erforderlich ist, weil sie voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringen.

Für den bayerischen öffentlichen, also insbesondere staatlichen und kommunalen Bereich gibt der Bayerische Landesbeauftragte für den Datenschutz auf Basis dieser Rechtsgrundlage die folgende, **nicht abschließende** Liste von Verarbeitungsvorgängen (**„Bayerische Blacklist"**) heraus.

Die vorliegende Bayerische Blacklist orientiert sich an den von der europäischen Datenschutzgruppe nach Artikel 29 veröffentlichten Leitlinien zur Datenschutz-Folgenabschätzung[1] (im Folgenden: Leitlinien), die der Europäische Datenschutzausschuss gebilligt hat. Sie ergänzt und konkretisiert diese Leitlinien sowie Art. 35 Abs. 3 DSGVO; dabei berücksichtigt sie auch die gemeinsame deutsche Liste gemäß Art. 35 Abs. 4 DSGVO für den nicht öf-

[1] Datenschutzgruppe nach Artikel 29, 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), im Internet abrufbar auf https://www.datenschutz-bayern.de in der Rubrik „Datenschutzreform 2018 – Orientierungs- und Praxishilfen – Datenschutz-Folgenabschätzung".

fentlichen Bereich (DSK-Liste) sowie die Auffassung des Europäischen Datenschutzausschusses zu dieser Liste.[2]

Nach den Leitlinien müssen folgende neun Kriterien (DSFA-Kriterien) berücksichtigt werden, um Verarbeitungsvorgänge zu ermitteln, für die aufgrund ihres hohen Risikos eine Datenschutz-Folgenabschätzung erforderlich ist:

(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 Personen,

(8) innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen,

(9) betroffene Personen werden an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags gehindert.

Die in der nachfolgenden Bayerischen Blacklist genannten Fallgruppen, in welchen eine Datenschutz-Folgenabschätzung erforderlich ist, werden durch Beispiele ergänzt und weiter konkretisiert.

Die **Bayerische Blacklist** erhebt **keinen Anspruch auf Vollständigkeit**, sondern soll das Bewusstsein für typische folgenabschätzungspflichtige Verarbeitungsvorgänge schärfen. Sie wird zu gegebener Zeit im erforderlichen Umfang aktualisiert werden.

[2] European Data Protection Board, Opinion 5/2018 on the draft list of the competent supervisory authorities of Germany regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR), im Internet abrufbar auf https://www.datenschutz-bayern.de in der Rubrik „Datenschutzreform 2018 – Orientierungs- und Praxishilfen – Datenschutz-Folgenabschätzung“ (bislang nur in englischer Sprache).

Bayerische Blacklist

	Fallgruppen	Beispiele	Kriterien[3]
1	**DSGVO-Fallgruppe „Bewertung persönlicher Aspekte“:** Systematische und umfassende 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	– Für den bayerischen öffentlichen Bereich derzeit kein Beispiel ersichtlich	Art. 35 Abs. 3 Buchst. a DSGVO
2	**DSGVO-Fallgruppe „umfangreiche Verarbeitung von Daten im Sinn von Art. 9 Abs. 1 und Art. 10 DSGVO“:** Umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Art. 9 Abs. 1 DSGVO oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DSGVO	– Beihilfebearbeitung durch das Landesamt für Finanzen, die Landeshauptstadt München oder durch Stellen mit vergleichbar umfangreicher Beihilfebearbeitung – Verfahren zur medizinischen Begutachtung (z. B. Pflegebegutachtung beim Medizinischen Dienst der Krankenversicherung) – Folgende Stellen mit Fachverfahren, die umfangreich Gesundheitsdaten verarbeiten: • Gesundheitsamt • Kassenärztliche Vereinigung • Krankenhaus • Krankenversicherung • Krebsregister • Landesweites Labor für Infektionsschutz • Rentenversicherung • Rettungsdienst • Stelle für Versorgungsforschung – Big Data im Gesundheitswesen – Umfangreiche Biobanken	Art. 35 Abs. 3 Buchst. b DSGVO
3	**DSGVO-Fallgruppe „Überwachung“:** Systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche	– Durchgängige Videoüberwachung des öffentlichen Personennahverkehrs in Großstädten	Art. 35 Abs. 3 Buchst. c DSGVO

[3] Maßgebliche DSFA-Kriterien und/oder einschlägige Fallgruppe des Art. 35 Abs. 3 DSGVO.

Bayerische Blacklist

	Fallgruppen	Beispiele	Kriterien[3]
4	**Biometrische Daten:** Verarbeitung biometrischer Daten zur eindeutigen Identifizierung natürlicher Personen, wenn zusätzlich mindestens ein weiteres DSFA-Kriterium vorliegt	– Einsatz biometrischer Systeme (z. B. Fingerabdruck, Sprachanalyse, Gesichtserkennung) zur Zutrittskontrolle für Beschäftigte oder für Bezahlungszwecke in Schulkantinen – Umfangreiche Verarbeitung der auf einem Ausweis (z. B. Personalausweis mit Fingerabdrucks-Daten) gespeicherten biometrischen Daten	(4) | zudem mindestens ein weiteres DSFA-Kriterium [ggf. Art. 35 Abs. 3 Buchst. b DSGVO]
5	**Genetische Daten:** Verarbeitung genetischer Daten im Sinne von Art. 4 Nr. 13 DSGVO, wenn zusätzlich mindestens ein weiteres DSFA-Kriterium vorliegt	– Eine Klinik setzt DNA-Tests zur Früherkennung vererblicher Krankheiten bei Neugeborenen ein – Genetische Untersuchungen im Rahmen medizinischer Forschung, bei der personenbezogene Daten aus mehreren Verarbeitungsvorgängen zusammengeführt werden	(4) | zudem mindestens ein weiteres DSFA-Kriterium [ggf. Art. 35 Abs. 3 Buchst. b DSGVO]
6	**Aufenthaltsbestimmung:** Systematische Verarbeitung von personenbezogenen Daten über den Aufenthalt von natürlichen Personen, die umfangreich ist oder schutzbedürftige Personen betrifft	– Verkehrsstromanalyse auf Grundlage von Standortdaten des öffentlichen Mobilfunknetzes oder von KFZ-Kennzeichen, auch wenn eine Anonymisierung stattfindet	(3) | (5) oder (7) [ggf. Art. 35 Abs. 3 Buchst. c DSGVO]
7	**Beschäftigte:** Umfangreiche Verarbeitung von personenbezogenen Daten über das Verhalten von Beschäftigten während der Arbeitszeit, die zur Bewertung ihrer Arbeitstätigkeit derart eingesetzt werden kann, dass sich Rechtsfolgen für betroffene Personen ergeben oder diese in anderer Weise erheblich beeinträchtigt werden	– Geolokalisierung von Beschäftigten während eines erheblichen Teils der Arbeitszeit	(1) | (5) | (7) | ggf. (3) [ggf. Art. 35 Abs. 3 Buchst. a DSGVO]
8	**Personalverwaltung:** Umfangreiche Verarbeitung von Personalaktendaten, die auch vertrauliche oder höchstpersönliche Daten betrifft	– Personal- und Stellenverwaltungssystem des Freistaates Bayern (VIVA) – Personal- und Stellenverwaltungssystem der Landeshauptstadt München (paul@)	(4) | (5) | (7) [ggf. Art. 35 Abs. 3 Buchst. b DSGVO]
9	**Künstliche Intelligenz (KI):** Einsatz von KI zur Verarbeitung personenbezogener Daten zur Steuerung der Interaktion mit den betroffenen Personen oder zur Bewertung persönlicher Aspekte der betroffenen Personen	– Nutzung eines Portals zur Personalgewinnung, in dem ein KI-System mit (potenziellen) Bewerberinnen und Bewerbern interagiert und/oder die Bewerberauswahl unterstützt – Nutzung von KI-unterstützter Bilderkennung für die Erkennung von Tumoren und für die medizinische Entscheidungsfindung	(6) | (8) | ggf. auch (1) und/oder (2) [ggf. Art. 35 Abs. 3 Buchst. a DSGVO]

	Fallgruppen	Beispiele	Kriterien[3]
10	**Persönlichkeitsbewertung mittels Video- oder Audio-Daten:** Automatisierte Auswertung von Video- oder Audio-Aufnahmen zur Bewertung persönlicher Aspekte der betroffenen Personen	– Automatisierte Auswertung von Mitarbeitergesprächen durch ein kommunales Call Center	(1) | (8) [ggf. Art. 35 Abs. 3 Buchst. a DSGVO]
11	**Datenerhebung via Sensor/mobile Anwendung:** Verarbeitung von personenbezogenen Daten gemäß Art. 9 Abs. 1 und Art. 10 DSGVO – auch wenn sie nicht als „umfangreich" im Sinne des Art 35 Abs. 3 Buchst. b DSGVO anzusehen ist –, sofern eine nicht nur einmalige Datenerhebung mittels der innovativen Nutzung von Sensoren oder mobilen Anwendungen stattfindet und diese Daten von einer zentralen Stelle empfangen und aufbereitet werden	– Online-Überwachung des Gesundheitszustands mittels Implantaten und zentraler Datenspeicherung, z. B. Insulinpumpen, Herzschrittmacher	(4) | (8)
12	**Leistungsfähigkeit:** 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 Buchst. b DSGVO anzusehen ist –, sofern die Daten durch die Anbieter neuer Technologien dazu verwendet werden, die Leistungsfähigkeit der Personen zu bestimmen	– Angebot von Fitness-Tracker-Armbändern, mit denen Gesundheitsdaten von Personen analysiert und online verarbeitet werden, durch eine öffentliche Krankenkasse	(1) | (4) | (8)
13	**Statistik:** Umfangreiche Verarbeitung inklusive Anonymisierung vertraulicher oder höchstpersönlicher Daten im Rahmen der amtlichen Statistik oder zum Zweck der Übermittlung an Dritte	– Zusammenführung zur Erstellung einer Statistik der Todesursachen in Bayern – Mikrozensus – Zensus	(4) | (5) | (6) [ggf. Art. 35 Abs. 3 Buchst. b DSGVO]
14	**IT-Sicherheitslösungen:** Umfangreiche Verarbeitung personenbezogener Daten im Rahmen technischer und/oder organisatorischer innovativer (IT-)Sicherheitslösungen	– Einsatz einer innovativen Softwarelösung zum Schutz vor Cyberattacken, die auch hinsichtlich personenbezogener Daten alle Datenflüsse detailliert kontrolliert oder/und Verschlüsselungen aufbricht	(5) | (8)
15	**Rechtswesen:** Verarbeitung von Daten bei Gerichten, bei Gerichtsvollziehern, bei Registern, die von Gerichten geführt werden, bei Notaren sowie bei Rechtsanwalts- oder Notarkammern, sofern die Verarbeitung mindestens zwei der nachfolgenden Merkmale erfüllt: – sie ist umfangreich, – sie umfasst vertrauliche oder höchstpersönliche Daten, – sie umfasst Daten von schutzbedürftigen betroffenen Personen	– Vorgangsverwaltungssysteme bei Betreuungs- und größeren Sozialgerichten	je nach Konstellation (4) | (5) | (7) [ggf. Art. 35 Abs. 3 Buchst. b DSGVO]

Bayerische Blacklist

	Fallgruppen	Beispiele	Kriterien[3]
16	**Schutzbedürftige Personen:**		
	Datenverarbeitung bezüglich schutzbedürftiger Personen, falls diese Verarbeitung vertrauliche oder höchstpersönliche Daten umfasst oder die Verarbeitung umfangreich ist	– Fachverfahren für die Gewährung von Leistungen für schwerbehinderte und diesen gleichgestellten behinderten Menschen – Fachverfahren für die Kinder- und Jugendhilfe zur Verarbeitung von Hilfedaten – Verwaltung von Plätzen in Kindertageseinrichtungen, soweit Daten elektronisch verarbeitet werden, die über die Gesundheit eines Kindes und/oder die Vermögensverhältnisse seiner Eltern Auskunft geben – Umfangreiche Verarbeitung personenbezogener Daten von minderjährigen Schülerinnen und Schülern im Rahmen der Schulverwaltung – Automatisierte Videoüberwachung von Krankenhauszimmern bei Suizidgefährdung	(7) | (4) oder (5) [ggf. Art. 35 Abs. 3 Buchst. b DSGVO]
17	**Zentralverfahren für Leistungsverwaltung:**		
	Umfangreiche Verarbeitung personenbezogener Daten im Rahmen der Leistungsverwaltung durch zentralisierte Fachverfahren, wenn zusätzlich mindestens ein weiteres DSFA-Kriterium vorliegt	– Bayerisches Landespflegegeld – Bayerische Opferentschädigung – Zentrale InVeKoS Datenbank (ZID) Deutschland für die Verwaltung der Zahlungsansprüche landwirtschaftlicher Betriebsinhaberinnen und Betriebsinhaber – Europäischer Sozialfonds (ESF)	(5) | zudem mindestens ein weiteres DSFA-Kriterium
18	**Profilbildung auf Basis von Sozial- oder Gesundheitsdaten:**		
	Verarbeitung umfasst die Bewertung oder Einstufung auf der Grundlage von Sozial- und/oder Gesundheitsdaten der betroffenen Personen	– Personenbezogene Profilbildung auf der Grundlage eines Fachverfahrens einer öffentlichen Krankenversicherung, das eine Vielzahl von Gesundheitsdaten der Versicherten verarbeitet – Verfahren für Antrag auf Feststellung des Grades einer Behinderung (ZBFS)	(1) | (4) [ggf. Art. 35 Abs. 3 Buchst. b DSGVO]
19	**Sozialdaten:**		
	Umfangreiche Verarbeitung von Sozialdaten	– Folgende Stellen mit Fachverfahren, die umfangreich Sozialdaten verarbeiten: • Jobcenter • Sozialamt – Fachverfahren für die Schuldnerberatung bei Mittel- und Großstädten sowie vergleichbaren Kommunen und bei landesweiten Verfahren	(4) | (5) | ggf. (1) [ggf. Art. 35 Abs. 3 Buchst. b DSGVO]

	Fallgruppen	Beispiele	Kriterien[3]
		– Fachverfahren für die Suchtberatung bei Mittel- und Großstädten sowie vergleichbaren Kommunen und bei landesweiten Verfahren	
20	**Kommunale Fachverfahren:**		
	Umfangreiche Verarbeitung vertraulicher oder höchstpersönlicher Daten durch kommunale Fachverfahren	– Verarbeitung von Personalausweis- und Passanträgen sowie der jeweiligen Register bei Mittel- und Großstädten sowie vergleichbaren Kommunen und bei landesweiten Verfahren – Verarbeitung der Meldedaten, Melderegister und Spiegelregister von Mittel- und Großstädten sowie vergleichbaren Kommunen und bei landesweiten Verfahren – Verfahren zur Führung von Personenstandsregistern von Mittel- und Großstädten sowie vergleichbaren Kommunen und bei landesweiten Verfahren – Verfahren zur Führung von Fahrerlaubnisregistern von Mittel- und Großstädten sowie vergleichbaren Kommunen und bei landesweiten Verfahren – Bereitstellung von Daten durch die AKDB für einen bayernweiten Melderegisterabgleich	(4) | (5) [ggf. Art. 35 Abs. 3 Buchst. b DSGVO]
21	**Drittländer:**		
	Umfangreiche und innovative Verarbeitung vertraulicher oder höchstpersönlicher Daten in Drittländern	– Umfangreiche Verarbeitung vertraulicher oder höchstpersönlicher Daten außerhalb der Europäischen Union und des Europäischen Wirtschaftsraums mittels Cloud Computing, sofern rechtlich zulässig	(4) | (5) | (8) [ggf. Art. 35 Abs. 3 Buchst. b DSGVO]