Entscheidung über die Notwendigkeit einer Datenschutzfolgenabschätzung

Gemäß Artikel 35 DS-GVO

(Dieser Text basiert auf einem Text der Datenschutzkonferenz.)

Auch bei einer rechtmäßigen Verarbeitung personenbezogener Daten entstehen Risiken für die betroffenen Personen. Deswegen sieht die DS-GVO unabhängig von sonstigen Voraussetzungen für die Verarbeitung vor, dass durch geeignete Abhilfemaßnahmen (insbesondere durch technische und organisatorische Maßnahmen (TOMs)) diese Risiken eingedämmt werden. Die Datenschutzfolgenabschätzung (DSFA) analysiert dazu die Risiken und die Schutzmaßnahmen.

# Was ist eine Datenschutz-Folgenabschätzung nach DS-GVO?

Eine DSFA ist ein spezielles Instrument zur Beschreibung, Bewertung und Eindämmung von Risiken für die Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten. Die DSFA ist durchzuführen, „wenn die Form der Verarbeitung, insbesondere bei der Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko zur Folge hat“. Sie befasst sich insbesondere mit Abhilfemaßnahmen, durch die der Schutz personenbezogener Daten sichergestellt und die Einhaltung der Verordnung nachgewiesen werden kann (Art. 35 Abs. 1, 7 DS-GVO sowie ErwGr. 84, 90).

# Erforderlichkeit einer DSFA

Ob eine DSFA durchzuführen ist, ergibt sich aus einer Abschätzung der Risiken der Verarbeitungsvorgänge („Schwellwertanalyse“). Ergibt diese ein voraussichtlich hohes Risiko, dann ist eine DSFA durchzuführen. Wird festgestellt, dass der Verarbeitungsvorgang kein hohes Risiko aufweist, dann ist eine DSFA nicht zwingend erforderlich. In jedem Fall ist die Entscheidung über die Durchführung oder Nichtdurchführung der DSFA mit Angabe der maßgeblichen Gründe für den konkreten Verarbeitungsvorgang schriftlich zu dokumentieren.

Art. 35 Abs. 3 DS-GVO benennt einige Faktoren, die wahrscheinlich zu einem hohen Risiko i. S. d. Art. 35 Abs. 1 DS-GVO führen. Aufbauend auf den Leitlinien der Artikel-29-Datenschutzgruppe werden die Datenschutzaufsichtsbehörden eine nicht-abschließende Liste mit Verarbeitungstätigkeiten, bei denen eine DSFA durchzuführen ist, veröffentlichen. Auch zur Durchführung der Schwellwertanalyse werden künftig Hinweise zur Verfügung gestellt.

# Zeitpunkt der Durchführung einer DSFA

Eine DSFA ist vor der Aufnahme der zu betrachtenden Verarbeitungsvorgänge durchzuführen. Auch bereits bestehende Verarbeitungsvorgänge können unter die Pflicht einer DSFA fallen. Da eine DSFA meist nicht ad hoc in wenigen Tagen erstellt werden kann, muss sie rechtzeitig, beispielsweise unterstützt durch ein allgemeines Datenschutz-Managementsystem, auf den Weg gebracht werden.

# Kriterien zur Beurteilung eines hohen Risikos das eine DSFA erforderlich macht

Um zu beurteilen, ob voraussichtlich ein hohes Risiko vorliegt können nach Artikel 29 Gruppe/Europäischem Datenschutzausschuss (WP248), folgende Kriterien herangezogen werden:

|  |  |  |
| --- | --- | --- |
|  | Verarbeitungen um zu Bewerten oder Einzustufen, darunter das Erstellen von Profilen und Prognosen, insbesondere auf der Grundlage von *„Aspekten, die die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, die Zuverlässigkeit oder das Verhalten, den Aufenthaltsort oder Ortswechsel der Person betreffen“* (ErwG 70 und 91 DS-GVO) | Hierfür seien zur Veranschaulichung folgende drei Beispiele genannt: 1) eine Biotechnologieforschung, bei dem man sich zwecks genetischer Tests direkt an Verbraucher wendet, um die Erkrankungs-/Gesundheitsrisiken abschätzen bzw. prognostizieren zu können, 2) Forschung bei der zum Ausschluss Probanden hinsichtlich bestimmter medizinischer Indikationen untersucht werden. |
|  | Automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung: Verarbeitung, auf deren Grundlage für Betroffene Entscheidungen getroffen werden sollen, „*die Rechtswirkung gegenüber natürlichen Personen entfalten*“ oder diese „*in ähnlich erheblicher Weise beeinträchtigen*“ (Artikel 35 Absatz 3 Buchstabe a).  | So kann die Verarbeitung beispielsweise zum Ausschluss oder zur Benachteiligung von Personen führen. Verarbeitungsvorgänge, die keine oder wenige Auswirkungen auf Personen haben, erfüllen nicht dieses spezielle Kriterium. Z.B. Plagiatssoftware, oder Verarbeitungen, die die Studienleistung automatisiert beurteilen könnten hier in Frage kommen. |
|  | Systematische Überwachung: Verarbeitungsvorgänge, die die Beobachtung, Überwachung oder Kontrolle von Betroffenen zum Ziel haben und auf beispielsweise über Netzwerke erfasste Daten oder auf „*eine systematische [...] Überwachung öffentlich zugänglicher Bereiche*“ (Artikel 35 Absatz 3 Buchstabe c) zurückgreifen. | Diese Form der Überwachung stellt ein Kriterium dar, weil die personenbezogenen Daten möglicherweise in Situationen erfasst werden, in denen die Betroffenen unter Umständen nicht wissen, wer ihre Daten erfasst und wie die Daten verwendet werden. Darüber hinaus kann es vorkommen, dass die Betroffenen keine Möglichkeit haben, eine solche Verarbeitung ihrer in der Öffentlichkeit (oder in öffentlich zugänglichen Bereichen) erfassten Daten zu verhindern. |
|  | Vertrauliche Daten oder höchst persönliche Daten: Hierzu zählen besondere Kategorien personenbezogener Daten (Art. 9 z. B. Informationen über die politischen Meinungen von Einzelpersonen) sowie personenbezogene Daten über strafrechtliche Verurteilungen oder Straftaten (Artikel 10)..  | Hierfür seien als Beispiele zunächst Gesundheitsdaten oder Daten über politische Einstellungen gemeint. Darüber hinaus gibt es weitere Datenkategorien, die zwar nicht in den DS-GVO-Bestimmungen aufgeführt sind, jedoch die möglichen Risiken für die Rechte und Freiheiten von Personen erhöhen können. Diese personenbezogenen Daten gelten als vertraulich (im gängigen Sinne des Wortes), da sie mit häuslichen und privaten Aktivitäten verknüpft sind (wie etwa die elektronische Kommunikation, deren Vertraulichkeit geschützt werden muss), sich auf die Ausübung eines der Grundrechte auswirken (wie etwa Standortdaten, deren Erfassung die Freizügigkeit in Frage stellt) oder die Verletzung derselben mit ernsthaften Konsequenzen für den Alltag des Betroffenen einhergeht (wie etwa Finanzdaten, die für den Zahlungsbetrug missbraucht werden könnten). In diesem Zusammenhang kann es von Bedeutung sein, ob die Daten durch den Betroffenen oder durch Dritte bereits öffentlich zugänglich gemacht worden sind. Die öffentliche Zugänglichkeit personen­bezogener Daten kann als bestimmender Faktor gelten, wenn beurteilt werden soll, ob eine weitere Nutzung der Daten für bestimmte Zwecke vorgesehen war. In dieses Kriterium können auch Daten wie persönliche Dokumente, E-Mails, Tagebücher, Notizen aus E-Readern mit Notizfunktion sowie über Lifelogging-Anwendungen erfasst werden, fallen. |
|  | Datenverarbeitung in großem Umfang: Zwar ist „in großem Umfang“ in der DSGVO nicht definiert, aber Erwägungsgrund 91 liefert einige Hinweise.  | Bei der Beurteilung ob ein großer Umfang erreicht wird, sollten folgende Faktoren berücksichtigt werden: 1. Zahl der Betroffenen, entweder als konkrete Anzahl oder als Anteil der entsprechenden Bevölkerungsgruppe;
2. verarbeitete Datenmenge bzw. Breite der unterschiedlichen verarbeiteten Datenelemente;
3. Dauer oder Dauerhaftigkeit der Datenverarbeitung;
4. geographisches Ausmaß der Datenverarbeitung.
 |
|  | Abgleichen oder Zusammenführen von Datensätzen | Zum Beispiel solcher Datensätze, die aus zwei oder mehreren Datenverarbeitungsvorgängen stammen, die zu unterschiedlichen Zwecken und/oder von verschiedenen für die Datenverarbeitung Verantwortlichen durchgeführt wurden, und zwar in einer Weise, die über die vernünftigen Erwartungen der Betroffenen hinausgeht. |
|  | Daten zu schutzbedürftigen Betroffenen (Erwägungsgrund 75): Die Verarbeitung dieser Art von Daten stellt ein Kriterium dar, weil zwischen den Betroffenen und dem für die Datenverarbeitung Verantwortlichen ein größeres Machtungleichgewicht vorliegt; d. h. den Personen ist es unter Umständen nicht ohne Weiteres möglich, der Verarbeitung ihrer Daten zuzustimmen bzw. zu widersprechen oder ihre Rechte auszuüben.  | Als schutzbedürftige Betroffene gelten beispielsweise folgende Bevölkerungs­gruppen: 1. Kinder (bei ihnen kann nicht davon ausgegangen werden, dass sie in der Lage sind, der Verarbeitung ihrer Daten wissentlich und überlegt zu widersprechen bzw. zuzustimmen),
2. Arbeitnehmer (in hohem Umfang der v),
3. Teile der Bevölkerung mit besonderem Schutzbedarf (psychisch Kranke, Asylbewerber, Senioren, Patienten *usw*.) und Betroffene in Situationen, in denen ein ungleiches Verhältnis zwischen der Stellung des Betroffenen und der des für die Verarbeitung Verantwortlichen vorliegt.
 |
|  | Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen, wie etwa die Kombination aus Fingerabdruck- und Gesichtserkennung zum Zwecke einer verbesserten Zugangskontrolle *usw*. von Personen auswirken und somit eine DSFA obligatorisch machen.  | Aus der DSGVO (Artikel 35 Absatz 1 und Erwägungsgründe 89 und 91) wird deutlich, dass der Einsatz einer neuen Technologie, die „*entsprechend dem jeweils aktuellen Stand der Technik*“ (Erwägungsgrund 91) als solche einzuordnen ist, der Grund für die Notwendigkeit einer DSFA sein kann. Das liegt daran, dass der Einsatz einer solchen Technologie mit neuartigen Formen der Datenerfassung und -nutzung einhergehen kann, was möglicherweise ein hohes Risiko für die Rechte und Freiheiten von Personen mit sich bringt. Schließlich sind die persönlichen und gesellschaftlichen Folgen, die der Einsatz einer neuen Technologie haben kann, kaum absehbar. Kann ein für die Datenverarbeitung Verantwortlicher auf eine DSFA zurückgreifen, kann er diese Risiken besser verstehen und bearbeiten. Beispielsweise könnten sich einige Anwendungen des „Internet der Dinge“ erheblich auf den Alltag und das Privatleben |
|  | Fälle, in denen die Verarbeitung an sich *„die betroffenen Personen an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags hindert“* (Artikel 22 und Erwägungsgrund 91). Hierzu zählen Verarbeitungsvorgänge, mit deren Hilfe Betroffenen der Zugriff auf eine Dienstleistung oder der Abschluss eines Vertrags gestattet, geändert oder verwehrt werden soll.  | Hierfür sei als Beispiel eine Bank genannt, die eine von Kreditauskunfteien betriebene Datenbank nach ihren Kunden durchsucht, um über Kreditvergaben zu entscheiden. |

Erfüllt ein Verarbeitungsvorgang **zwei** dieser Kriterien, muss der für die Datenverarbeitung Verantwortliche in den meisten Fällen zu dem Schluss kommen, dass eine DSFA obligatorisch ist. Nach Auffassung der WP29 nimmt die Wahrscheinlichkeit, dass ein Verarbeitungsvorgang ein hohes Risiko für die Rechte und Freiheiten von Betroffenen mit sich bringt und somit eine DSFA erforderlich ist (und zwar unabhängig von den Maßnahmen, die der für die Verarbeitung Verantwortliche ins Auge fasst), im Allgemeinen immer weiter zu, je mehr Kriterien dieser Vorgang erfüllt.