|  |
| --- |
| Anlage 2 DatSch Ordner 1 Register 6  Muster Umsetzung Risikobewertung |

|  |  |
| --- | --- |
|  | **Verarbeitungstätigkeiten gem. Artikel 30 Abs. 1 DSGVO** |
|  | **Verarbeitungstätigkeiten Auftragsverarbeiter gem. Artikel 30 Abs. 2 DSGVO** |

|  |  |
| --- | --- |
| **lfd. Nr.:** |  |
| Benennung: |  |
| Datum der Einführung: |  |
| Datum der Risikobewertung: |  |

Anlage: Verarbeitungstätigkeiten gem. Artikel 30 Abs. 1 oder 2 DSGVO

Risikobewertung nach Vorgaben DSGVO Artikel 35 Absatz 1 und Artikels 29 der Europäischen Datenschutzrichtlinie 95/46/EG.

1. Umsetzung der Risikobewertung
2. Liegen folgende Risikokriterien für ein hohes Risiko für die Rechte und Freiheiten einer natürlichen Person vor:

|  |  |
| --- | --- |
| **Prüfkriterien** | **JA** |
| * **Ausführung Scoring / Profiling / Tracking** * **Scoring**   Der Begriff „Scoring“ stammt aus dem Englischen und leitet sich von „to score“ bzw. „score“ ab, was punkten bzw. Punktestand bedeutet. Unter ihm versteht man mathematisch-statistische Verfahren, mit denen auf Grund von Erfahrungswerten aus der Vergangenheit Wahrscheinlichkeitswerte für ein bestimmtes zukünftiges Verhalten oder zukünftige Ereignisse ermittelt werden.  **Profiling**  (englisch *profiling*) bezeichnet die Erstellung, Aktualisierung und Verwendung von Profilen durch Sammlung von (auch im Internet gewonnener) Daten, sowie deren anschließende Analyse und Auswertung, zum Zwecke der Identifikation und Überwachung von Personen, zur Leistungsmessung (Scoring), zur Optimierung und Vorhersage des (Direkt) marketings, oder zum Zwecke der Wahl-, Verhaltens- und Meinungsbeeinflussung.  **Tracking** (dt. für den statischen [retrospektiven] Anwendungsfall gleichbedeutend mit Spurbildung, für den dynamischen Anwendungsfall [mitlaufend, online] gleichbedeutend mit Nachführung) umfasst alle Bearbeitungsschritte, die der gleichzeitigen Verfolgung von (bewegten) Objekten dienen. Davon unterschieden wird das *Tracing*, das eine zeitlich versetzte Verfolgung anhand von Aufzeichnungen betrifft, z. B. in der Programmierung als Ablaufverfolgung. Die Abgrenzung ist aber nicht einheitlich, so spricht man z. B. von einem GPS-Tracking unabhängig davon, ob die Verfolgung (Auswertung) gleichzeitig oder nachträglich erfolgt. |  |
| * **Automatische-Entscheidungen, die zu rechtlichen Folgen für die Betroffenen** * **Führen.**   Wenn die Verarbeitung von Daten beispielsweise dazu führt, dass jemand einen Vertrag nicht abschließen kann. |  |
| * **Systematische Überwachung** * Verarbeitungsvorgänge, die Betroffene beobachten, überwachen oder kontrollieren sollen und auf beispielsweise über Netzwerke erfasste Daten oder auf die Überwachung öffentlich zugänglicher Bereiche zurückgreifen. |  |
| * **Sensible Daten (besondere personenbezogene Daten aus Art. 9 DSGVO)** * Beispiele sind ein Krankenhaus, das die Krankenakten seiner Patienten archiviert, oder ein Privatdetektiv, der Akten zu Straftätern führt. * Sensible Daten sind: Namen (Vor- Zu und Geburtsnamen)**,** Geburtsdaten (Datum, Ort)**,** Kontaktdaten (Adresse, Telekom)**,** Körperliche Merkmale (Größe, Gewicht)**,** Geistige Zustände**,** Krankheiten**,** Arbeitgeberdaten**,** Familiendaten**,** Standortdaten**,** Nutzungsdaten**,** Steuerliche Merkmale**,** Handlungen**,** Bankverbindungen**,** Freundschaftsbeziehungen**,** Werturteile**,** Beruflicher Wertegang**,** Bewerbungen. |  |
| * **Daten die in großem Umfang verarbeitet werden (Kriterium: Anzahl der Betroffenen, Menge der Daten etc.)** * Es gibt viele Betroffene oder es werden sehr viele Daten verarbeitet. |  |
| * **Zusammenführen/ kombinieren von Daten die durch unterschiedliche Prozesse gewonnen wurden** * die durch unterschiedliche Prozesse gewonnen wurden und wenn die Betroffenen nicht damit rechnen können, dass die Daten zusammengeführt werden. |  |
| * **Daten geschäftsunfähiger oder beschränkt geschäftsfähiger Betroffener** * Das umfasst Kinder und psychisch Kranke. Auch Arbeitnehmer, Asylbewerber, Senioren oder Patienten fallen darunter, sofern ein ungleiches Verhältnis zwischen der Stellung des Betroffenen und der Stellung des Verantwortlichen für die Datenverarbeitung besteht. |  |
| * **Einsatz neuer Technologien oder biometrischer Verfahren** * zum Beispiel die Kombination aus Fingerabdruck- und Gesichtserkennung zum Zweck einer verbesserten Zugangskontrolle. |  |
| * **Datentransfer in Länder außerhalb der EU/EWR** * Datentransfer in Ländern außerhalb der EU. Datenspeicherung, Auswertung, Auftragsverarbeitungen. |  |
| * **Die Datenverarbeitung hindert Betroffene an der Rechtsausübung** * Beispiel: Eine Bank, die eine von Kreditauskunfteien betriebene Datenbank nach ihren Kunden durchsucht, um über Kreditvergaben zu entscheiden. |  |

1. Rechtliche Vorgaben durch Landesdatenschutzbehörden gemäß Artikel 35 Absatz 4 DSGVO

Hinweise: Die Liste der Landesdatenschutzbehörden wird ständig überarbeitet. Eine Prüfung vor Auswertung ist daher angeraten.

Stand: 01.09.2018

|  |  |
| --- | --- |
| **Prüfkriterien anhand der Verarbeitung** | **JA** |
| **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 |  |
| **Umfangreiche Verarbeitung von Daten** über den Aufenthalt von Personen |  |
| **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 |  |
| **Verarbeitung von Daten gemäß Art. 9 Abs. 1 und 10 DSGVO durch Auftragsverarbeiter**, denen von einem Gericht oder einer Verwaltungsbehörde eines Drittlands die Pflicht auferlegt werden kann, diese Daten entgegen Art. 48 DSGVO zu exportieren oder offenzulegen |  |
| **Mobile** und für die Betroffenen **intransparente optoelektronische Erfassung** öffentlicher Bereiche |  |
| **Mobile optisch-elektronische Erfassung** personenbezogener Daten in öffentlichen Bereichen, sofern die Daten aus ein oder mehreren Erfassungssystemen in großem Umfang zentral zusammengeführt werden. |  |
| **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 |  |
| **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 |  |
| **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 |  |
| **Erstellung umfassender Profile** über die Interessen, das Netz persönlicher Beziehungen oder die Persönlichkeit der Betroffenen |  |
| **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, 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** |  |
| **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, die Anwendung von Algorithmen einschließen, die für die Betroffenen nicht nachvollziehbar sind. |  |
| **Einsatz von künstlicher Intelligenz** zur Verarbeitung personenbezogener Daten zur Steuerung der Interaktion mit den Betroffenen oder zur Bewertung persönlicher Aspekte der Betroffenen |  |
| **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 |  |
| **Automatisierte Auswertung von Video- oder Audio-Aufnahmen** zur Bewertung der Persönlichkeit der Betroffenen |  |
| **Erhebung personenbezogener Daten** über Schnittstellen persönlicher elektronischer Geräte, die nicht gegen ein unbefugtes Auslesen geschützt sind, das die Betroffenen nicht erkennen können |  |
| **Erstellung umfassender Profile** über die Bewegung und das Kaufverhalten von Betroffenen |  |
| **Anonymisierung** von besonderen personenbezogenen 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 |  |
| **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 |  |
| **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. |  |
| **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 der innovativen Nutzung von Sensoren** oder mobilen Anwendungen stattfindet und diese Daten von einer zentralen Stelle empfangen und aufbereitet werden. |  |
| 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 |  |
| 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. |  |
| **Umfangreiche Datenerhebung bei Beschäftigten** mit dem Ziel oder zumindest der Möglichkeit der Verhaltens- und Leistungskontrolle im Arbeitsverhältnis |  |
| **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 durch zentrale Internetdienste |  |
| **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 Übertragung der Daten mittels digitaler Fernkommunikationsmittel erfolgt |  |

1. Freiwillige Erklärung zur Datenschutzfolgeabschätzung

|  |  |
| --- | --- |
| Umsetzung aufgrund vertraglicher Verpflichtungen |  |
| Umsetzung nach Vorgaben der Geschäftsführung |  |

1. **Ergebnis der Risikobewertung**

B 1) Auswertung

|  |  |  |  |
| --- | --- | --- | --- |
| **Nr.** | **Auswerteinhalte** | **Kriterium** | **Pflicht DSFA** |
| A 1 | Liegen folgende Risikokriterien für ein hohes Risiko für die Rechte und Freiheiten einer natürlichen Person vor | **2 Kriterien erfüllt** |  |
| A 2 | Rechtliche Vorgaben durch Landesdatenschutzbehörden gemäß Artikel 35 Absatz 4 DSGVO | **1 Kriterium erfüllt** |  |
| A 3 | Freiwillige Erklärung zur Datenschutzfolgeabschätzung | **1 Kriterium erfüllt** |  |

B 2) Ergebnis der Auswertung

|  |  |
| --- | --- |
|  | **Es besteht keine Pflicht zur Datenschutzfolgeabschätzung** |

Maßnahmen: Vorlage der Auswertung Dokumentieren und Vorlage bei der Geschäftsführung.

|  |  |
| --- | --- |
|  | **Es besteht die Pflicht zur Datenschutzfolgeabschätzung** |

Maßnahmen: Zusammenfassung der Risikobewertung als Anlage zur Datenschutzfolge-abschätzung. Umsetzung der Datenschutzfolgeabschätzung nach Anlage 3

Ordner 1 Register 6 Muster Umsetzung Datenschutzfolgeabschätzung

1. **Unterschrift Umsetzenden**

|  |  |
| --- | --- |
| Datum |  |
| Name |  |
| Vorname |  |

Unterschrift

|  |
| --- |
|  |

1. **Kenntnisnahme Geschäftsführung**

|  |  |
| --- | --- |
| Datum |  |
| Name |  |
| Vorname |  |

Unterschrift

|  |
| --- |
|  |

D 1 Anordnung der Geschäftsführung

|  |  |
| --- | --- |
|  | Ablage in der Datenschutzorganisation |
|  | Umsetzung der Datenschutzfolgeabschätzung trotz negativer Auswertung |
|  | Sonstiges: |