

ÜBERSICHT: WANN EINE DATENSCHUTZ-FOLGENABSCHÄTZUNG (DSFA) PFLICHT IST

| Nr. | Beschreibung der Verarbeitungstätigkeit | Typische Einsatzfelder | Beispiele |
|-----|---|---|--|
| 01 | <p>„Verarbeitung von biometrischen Daten zur eindeutigen Identifizierung natürlicher Personen, wenn mindestens ein weiteres folgendes Kriterium aus WP 248 Rev. 01 zutrifft:</p> <ul style="list-style-type: none"> • Daten zu schutzbedürftigen Betroffenen • Systematische Überwachung • Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen • Bewerten oder Einstufen (Scoring) • Abgleichen oder Zusammenführen von Datensätzen • Automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung • Betroffene werden an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags gehindert | <p>Verwendung von biometrischen Systemen zur Zutrittskontrolle oder für Abrechnungszwecke</p> | <p>Ein Unternehmen setzt flächendeckend Fingerabdrucksensoren zur Zutrittskontrolle für bestimmte Bereiche ein.</p> <p>Eine Schulkantine bietet den Schülern das „Bezahlen per Fingerabdruck“ an.</p> |
| 02 | <p>Verarbeitung von genetischen Daten im Sinne von Artikel 4 Nr. 13 DSGVO, wenn mindestens ein weiteres folgendes Kriterium aus WP 248 Rev. 01 zutrifft:</p> <ul style="list-style-type: none"> • Daten zu schutzbedürftigen Betroffenen • Systematische Überwachung • Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen • Bewerten oder Einstufen (Scoring) • Abgleichen oder Zusammenführen von Datensätzen • Automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung • Betroffene werden an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags gehindert | <p>Früherkennung von Erbkrankheiten</p> <p>Genetische Datenbanken zur Abstammungsforschung</p> | <p>Eine Klinik setzt DNA-Tests zur Früherkennung vererblicher Krankheiten bei Neugeborenen ein.</p> <p>Ein Unternehmen bietet einen Dienst an, über den Kunden die eigenen genetischen Daten mit denen Dritter abgleichen können, um mehr über die eigene Abstammung zu erfahren. Dazu pflegt das Unternehmen eine Datenbank mit genetischen Daten einer Vielzahl von Personen.</p> |
| 03 | <p>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 DSGVO handelt</p> | <p>Betrieb eines Insolvenzverzeichnisses</p> <p>Träger von großen sozialen Einrichtungen</p> <p>Große Anwaltssozietät</p> | <p>Ein Unternehmen bietet ein umfassendes Verzeichnis über Privatinsolvenzen an.</p> <p>Große Rechtsanwaltskanzlei, die im Schwerpunkt familienrechtliche Mandate betreut.</p> |
| 04 | <p>Umfangreiche Verarbeitung von personenbezogenen Daten über den Aufenthalt von natürlichen Personen</p> | <p>Fahrzeugdatenverarbeitung – Car Sharing / Mobilitätsdienste</p> <p>Fahrzeugdatenverarbeitung – Zentrale Verarbeitung der Messwerte oder Bilderzeugnisse von Umgebungssensoren</p> <p>Offline-Tracking von Kundenbewegungen in Warenhäusern, Einkaufszentren o. ä.</p> <p>Verkehrsstromanalyse auf der Grundlage von Standortdaten des öffentlichen Mobilfunknetzes</p> | <p>„Ein Unternehmen bietet einen Car-Sharing-Dienst oder andere Mobilitätsdienstleistungen an und verarbeitet hierfür insbesondere umfangreich Positions- und Abrechnungsdaten.</p> <p>Ein Unternehmen erhebt personenbezogene Daten, die Fahrzeuge über ihre Umgebung generieren und ermittelt daraus beispielsweise freie Parkplätze oder verbessert Algorithmen zum automatisierten Fahren.</p> <p>Ein Unternehmen verarbeitet die GPS-, Bluetooth- und/oder Mobilfunksignale von Passanten und Kunden, um die Laufwege und das Einkaufsverhalten nachverfolgen zu können.“</p> |

Übersicht: Wann eine Datenschutz-Folgenabschätzung (DSFA) Pflicht ist

| Nr. | Beschreibung der Verarbeitungstätigkeit | Typische Einsatzfelder | Beispiele |
|--|--|---|-----------|
| <p>05 Zusammenführung von personenbezogenen Daten aus verschiedenen Quellen und Verarbeitung der so zusammengeführten Daten, sofern:</p> <ul style="list-style-type: none"> • die Zusammenführung oder Verarbeitung 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 | <p>Fraud-Prevention-Systeme</p> <p>Scoring durch Auskunftsteien, Banken oder Versicherungen</p> | <p>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.</p> <p>Eine Auskunftstei 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.</p> | |
| <p>06 Mobile optisch-elektronische Erfassung personenbezogener Daten in öffentlichen Bereichen, sofern die Daten aus ein oder mehreren Erfassungssystemen in großem Umfang zentral zusammengeführt werden</p> | <p>Fahrzeugdatenverarbeitung – Umgebungssensoren</p> | <p>Ein Unternehmen erhebt personenbezogene Daten, die Fahrzeuge über ihre Umgebung generieren und ermittelt daraus beispielsweise freie Parkplätze oder verbessert Algorithmen zum automatisierten Fahren.</p> | |
| <p>07 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</p> | <p>Betrieb von Bewertungsportalen</p> <p>Inkassodienstleistungen – Forderungsmanagement</p> <p>Inkassodienstleistungen – Factoring</p> | <p>Ein Online-Portal bietet Nutzern die Möglichkeit an, Leistungen von Selbstständigen öffentlich feingranular zu bewerten. Online-Bewertungsportal bspw. für Ärzte, Selbstständige oder Lehrer.</p> <p>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 Auskunftsteien übermittelt.</p> <p>Ein Unternehmen lässt sich in großem Umfang Forderungen übertragen um diese auf eigenes Risiko geltend zu machen. Es verarbeitet hierfür insbesondere Vertragsdaten, Rechnungsdaten, Scoringdaten und Informationen über Vermögensverhältnisse von Schuldnern. Ggf. werden Daten an Auskunftsteien übermittelt.</p> | |
| <p>08 Umfangreiche Verarbeitung von 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</p> | <p>Einsatz von Data-Loss-Prevention-Systemen</p> <p>Geolokalisierung von Beschäftigten</p> | <p>Zentrale Aufzeichnung der Aktivitäten am Arbeitsplatz“ „Zentrale Aufzeichnung der Aktivitäten (z. B. Internetverkehr, Mailverkehr, Nutzung von Wechselmedien), um unerwünschtes Verhalten (z. B. Versand interner Dokumente) zu erkennen.</p> <p>Ein Unternehmen lässt Bewegungsprofile von Beschäftigten erstellen (per RFID, Handy-Ortung oder GPS), z. B. zur Sicherung von Personal oder wertvollem Eigentum oder zur Koordination im Außendienst.</p> | |
| <p>09 Erstellung umfassender Profile über die Interessen, das Netz persönlicher Beziehungen oder die Persönlichkeit der Betroffenen</p> | <p>Betrieb von Dating- und Kontaktportalen</p> <p>Betrieb von großen Sozialen Netzwerken</p> | <p>Ein Webportal erstellt Profile der Nutzer, um möglichst passende Kontaktvorschläge zu generieren.</p> | |

Übersicht: Wann eine Datenschutz-Folgenabschätzung (DSFA) Pflicht ist

| Nr. | Beschreibung der Verarbeitungstätigkeit | Typische Einsatzfelder | Beispiele |
|-----|---|--|--|
| 10 | <p>Zusammenführung von personenbezogenen Daten aus verschiedenen Quellen und der Verarbeitung der so zusammengeführten Daten, sofern:</p> <ul style="list-style-type: none"> • die Zusammenführung oder Verarbeitung 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, • der Entdeckung vorher unbekannter Zusammenhänge zwischen den Daten für nicht im Vorhinein bestimmte Zwecke dienen | <p>Big-Data-Analyse von Kundendaten, die mit Angaben aus Drittquellen angereichert wurden</p> | <p>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 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.</p> |
| 11 | <p>Einsatz von künstlicher Intelligenz zur Verarbeitung personenbezogener Daten zur Steuerung der Interaktion mit den Betroffenen oder zur Bewertung persönlicher Aspekte der betroffenen Person</p> | <p>Kundensupport mittels künstlicherIntelligenz</p> | <p>Ein Callcenter wertet automatisiert die Stimmungslage der Anrufer aus. Ein Unternehmen setzt ein System ein, welches mit Kunden interagiert und personenbezogene Daten analysiert.</p> |
| 12 | <p>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 substantziellen Zeitraum</p> | <p>Offline-Tracking von Kundenbewegungen in Warenhäusern, Einkaufszentren o. ä.</p> <p>Verkehrsstromanalyse auf der Grundlage von Standortdaten des öffentlichen Mobilfunknetzes</p> | <p>Ein Unternehmen verarbeitet die WLAN-, Bluetooth- oder Mobilfunksignale von Passanten und Kunden, um die Laufwege und das Einkaufsverhalten nachverfolgen zu können.</p> |
| 13 | <p>Automatisierte Auswertung von Video- oder Audio-Aufnahmen zur Bewertung der Persönlichkeit der Betroffenen</p> | <p>Telefongespräch-Auswertung mittels Algorithmen</p> | <p>Ein Callcenter wertet automatisiert die Stimmungslage der Anrufer aus.</p> |
| 14 | <p>Erstellung umfassender Profile über die Bewegung und das Kaufverhalten von Betroffenen</p> | <p>Erfassung des Kaufverhaltens unterschiedlicher Personenkreise zur Profilbildung und Kundenbindung unter Zuhilfenahme von Preisen, Preisnachlässen und Rabatten</p> | <p>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.</p> |
| 15 | <p>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</p> | <p>Anonymisierung von besonderen Arten personenbezogener Daten nach Artikel 9</p> | <p>Umfangreiche besondere personenbezogene Daten werden durch ein Apothekenrechenzentrum oder eine Versicherung anonymisiert und zu anderen Zwecken selbst verarbeitet oder an Dritte weitergegeben.</p> |
| 16 | <p>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</p> | <p>Einsatz von Telemedizin-Lösungen zur detaillierten Bearbeitung von Krankheitsdaten</p> | <p>Ein Arzt nutzt ein Webportal oder setzt eine App an, um mit Patienten mittels Videotelefonie zu kommunizieren und Gesundheitsdaten durch Sensoren beim Patienten (z.B. Blutzucker, Sauerstoffmaske,...) detailliert und systematisch zu erheben und zu verarbeiten.</p> |

Übersicht: Wann eine Datenschutz-Folgenabschätzung (DSFA) Pflicht ist

| Nr. | Beschreibung der Verarbeitungstätigkeit | Typische Einsatzfelder | Beispiele |
|-----|--|---|--|
| 17 | 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. |

Hinweise

1. Diese Liste ist nicht abschließend, sondern ergänzt die in den Absätzen 1 und 3 des Artikels 35 DSGVO enthaltenen allgemeinen Regelungen.

Allgemein gilt, dass für jede Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, die aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, vorab eine Datenschutz-Folgenabschätzung durchgeführt werden muss, insbesondere in den in Absatz 3 genannten Fällen.

2. Diese Liste orientiert sich an der allgemeinen, im Arbeitspapier 248 Rev. 1 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“ beschriebenen Vorgehensweise. Sie ergänzt und konkretisiert diese allgemeine Vorgehensweise.

Der Leitlinie sind folgende neun maßgebliche Kriterien aus WP 248 Rev. 01 zur Einordnung von Verarbeitungsvorgängen zu entnehmen:

- a) Vertrauliche oder höchst persönliche Daten
- b) Daten zu schutzbedürftigen Betroffenen
- c) Datenverarbeitung in großem Umfang
- d) Systematische Überwachung
- e) Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen
- f) Bewerten oder Einstufen (Scoring)
- g) Abgleichen oder Zusammenführen von Datensätzen
- h) Automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung
- i) Betroffene werden an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags gehindert