Entwurf

Verordnung der Datenschutzbehörde über Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist (DSFA-V)

Auf Grund des § 21 Abs. 2 des Datenschutzgesetzes (DSG), BGBl. I Nr. 165/1999, zuletzt geändert durch das Bundesgesetz BGBl. I Nr. 24/2018, wird verordnet:

Geltungsbereich

§ 1. Die Bestimmungen dieser Verordnung gelten für die Datenschutz-Folgenabschätzung, die gemäß Art. 35 Abs. 1 der Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. Nr. L 119 vom 4.5.2016 S. 1 (im Folgenden: DSGVO), vom Verantwortlichen durchzuführen ist.

Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist

§ 2. (1) Sofern die Verarbeitung rechtmäßig im Sinne des Art. 6 DSGVO erfolgt und keine Datenverarbeitung gemäß der Verordnung der Datenschutzbehörde über die Ausnahmen von der Datenschutz-Folgenabschätzung (DSFA-AV), BGBl. II Nr. 108/2018, vorliegt, ist nach Maßgabe der folgenden Bestimmungen jedenfalls eine Datenschutz-Folgenabschätzung durchzuführen.

(2) Eine Datenschutz-Folgenabschätzung ist durch den Verantwortlichen durchzuführen, wenn ein in Z 1 bis Z 7 genanntes Kriterium erfüllt ist:

1. Verarbeitungen, die eine Bewertung oder Einstufung natürlicher Personen – einschließlich des Erstellens von Profilen und Prognosen – umfassen für Zwecke, welche die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben und Interessen, die Zuverlässigkeit oder das Verhalten, den Aufenthaltsort oder Ortswechsel der Person betreffen und negative rechtliche, physische oder finanzielle Auswirkungen haben können.
2. Verarbeitungen von Daten, die zur Bewertung des Verhaltens und anderer persönlicher Aspekte von natürlichen Personen dienen und von Dritten dazu genutzt werden können, automatisierte Entscheidungsfindungen zu treffen, die Rechtswirkung gegenüber den bewerteten Personen entfalten, oder diese in ähnlich erheblicher Weise beeinträchtigen.
3. Verarbeitungsvorgänge, welche die Beobachtung, Überwachung oder Kontrolle von Betroffenen – insbesondere mittels Bild- und damit verbundenen Akustikdatenverarbeitungen – zum Ziel haben und
   a) über Netzwerke erfasste Daten betreffen oder auf eine systematische, umfangreiche Überwachung öffentlich zugänglicher Bereiche abzielen,
   b) öffentliche Orte, die gemäß § 27 Abs. 2 Sicherheitspolizeigesetz – SPG, BGBl. Nr. 566/1991, von einem nicht von vornherein bestimmten Personenkreis betreten werden können, erfassen,
   c) Straßen mit öffentlichem Verkehr, die gemäß § 1 Straßenverkehrsordnung 1960 (StVO 1960), BGBl. Nr. 159/1960, von jedermann unter den gleichen Bedingungen benützt werden können, erfassen,
   d) Örtlichkeiten, welche aufgrund eines Kontrahierungszwanges von jedermann betreten werden dürfen, erfassen,
   e) Örtlichkeiten, welche aufgrund des öffentlichen Interesses von jedermann betreten werden dürfen, erfassen,

f) unter Einsatz von mobilen Kameras zum Zweck der Vorbeugung oder Abwehr gefährlicher Angriffe im öffentlichen und nichtöffentlichen Raum erfolgen,

g) Bild- und Akustikverarbeitungen umfassen, die dem vorbeugenden Schutz von Personen oder Sachen auf privaten, zu Wohnzwecken dienenden Liegenschaften dienen, die nicht ausschließlich vom Verantwortlichen und von allen im gemeinsamen Haushalt lebenden Nutzungsberechtigten genutzt werden, oder

h) Kirchen, Gebetshäuser und andere Einrichtungen, die für die Religionsausübung genutzt werden, erfassen.

4. Verarbeitung von Daten unter Nutzung oder Anwendung neuer bzw. neuartiger Technologien oder organisatorischer Lösungen, welche die Abschätzung der Auswirkungen auf die Betroffenen und die gesellschaftlichen Folgen erschweren, insbesondere durch den Einsatz von künstlicher Intelligenz und die Verarbeitung biometrischer Daten, sofern die Verarbeitung nicht die bloße Echtzeitwiedergabe von Gesichtsbildern betrifft.
5. Verarbeitungsvorgänge von gemäß Art. 26 DSGVO gemeinsam für die Verarbeitung Verantwortlichen.
6. Zusammenführung und/oder Abgleich von Datensätzen aus zwei oder mehreren Verarbeitungen im Rahmen einer Datenverarbeitung, die zu unterschiedlichen Zwecken und/oder von verschiedenen Verantwortlichen durchgeführt wurden, die über die von einem Betroffenen üblicherweise zu erwartenden Verarbeitungen hinausgehen, sofern
   a) diese für Zwecke erfolgen, für welche nicht alle der zu verarbeitenden Daten direkt beim Betroffenen erhoben wurden, oder
   b) durch die Anwendung von Algorithmen Entscheidungen getroffen werden können, welche die betroffenen Personen in erheblicher Weise beeinträchtigen.
7. Verarbeitungsvorgänge im höchstpersönlichen Bereich von Personen, auch wenn die Verarbeitung auf einer Einwilligung beruht.

Im Zusammenhang mit Beschäftigungsverhältnissen gilt dies nicht, wenn eine Betriebsvereinbarung oder Zustimmung der Personalvertretung vorliegt. Als systematische Überwachung sind jene Vorgänge zu verstehen, die im Rahmen eines Systems oder vorab festgelegt, organisiert und methodisch erfolgen.

(3) Eine Datenschutz-Folgenabschätzung ist durch den Verantwortlichen durchzuführen, wenn ein Verarbeitungsvorgang zwei oder mehr der nachstehenden Kriterien erfüllt:

1. Verarbeitung von besonderen Kategorien personenbezogener Daten gemäß Art. 9 DSGVO,
2. Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DSGVO,
3. Erfassung von Standortdaten im Sinne des § 92 Abs. 3 Z 6 Telekommunikationsgesetz 2003 – TKG 2003, BGBl. I. Nr. 70/2003, die in einem Kommunikationsnetz oder von einem Kommunikationsdienst verarbeitet werden und die den geografischen Standort der Telekommunikationsendeinrichtung eines Nutzers eines öffentlichen Kommunikationsdienstes angeben, oder
4. die Verarbeitung von Daten zu schutzbedürftigen Betroffenen, wie unmündigen Minderjährigen, Arbeitnehmern, Patienten, psychisch Kranken und Asylwerbern.

Personenbezogene Bezeichnungen

§ 3. Bei den in dieser Verordnung verwendeten personenbezogenen Bezeichnungen gilt die gewählte Form für beide Geschlechter.

Verweisungen

§ 4. Verweisungen in dieser Verordnung auf andere Bundesgesetze oder auf Verordnungen sind als Verweisungen auf die jeweils geltende Fassung zu verstehen.

Inkrafttreten

§ 5. Diese Verordnung tritt mit Ablauf des Tages der Kundmachung im Bundesgesetzblatt in Kraft.

Erläuterungen

Allgemeiner Teil

Die Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. Nr. L 119 vom 4.5.2016 S. 1, (im Folgenden: DSGVO), gilt seit dem 25. Mai 2018.

Art. 35 Abs. 1 DSGVO erlegt allen Verantwortlichen die Pflicht auf, eine Datenschutz-Folgenabschätzung durchzuführen, wenn aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich mit einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen zu rechnen ist.

Gemäß Art. 35 Abs. 4 DSGVO hat die Aufsichtsbehörde eine Liste der Arten von Verarbeitungsvorgängen zu erstellen und veröffentlichen, für die eine Datenschutz-Folgenabschätzung gemäß Abs. 1 durchzuführen ist. Das Datenschutzgesetz (DSG), BGBl. I Nr. 165/1999, trat ebenfalls am 25. Mai 2018 in Kraft. § 18 DSG bestimmt die Datenschutzbehörde als nationale Aufsichtsbehörde nach der DSGVO und überträgt ihr gemäß § 21 Abs. 2 die Kompetenz, die Liste nach Art. 35 Abs. 4 DSGVO zu erstellen und im Wege einer Verordnung im Bundesgesetzblatt kundzumachen.

Nach der DSGVO müssen die für die Verarbeitung Verantwortlichen geeignete Maßnahmen ergreifen, um sicherzustellen – und den Nachweis dafür zu erbringen –, dass die Verarbeitung gemäß der DSGVO erfolgt, wobei sie unter anderem die „unterschiedliche Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen“ zu berücksichtigen haben. Die Vorgabe, dass die/der Verantwortliche unter bestimmten Voraussetzungen eine Datenschutz-Folgenabschätzung durchführen muss, ist vor dem Hintergrund ihrer allgemeinen Pflicht zu verstehen, eine geeignete Abschätzung der Risiken zu betreiben, welche die Verarbeitung personenbezogener Daten birgt.

Mit dem vorliegenden Entwurf werden Verantwortliche in ihrer Verpflichtung dahingehend unterstützt, dass in einem Kriterienkatalog jene Verarbeitungsvorgänge normiert werden, bei denen vom Vorliegen eines hohen Risikos für die Rechte und Freiheiten natürlicher Personen jedenfalls auszugehen ist und die folglich der Verpflichtung zur Durchführung einer Datenschutz-Folgenabschätzung unterliegen. Der Entwurf bildet das Pendant zu der mit BGBl. II Nr. 108/2018 kundgemachten Verordnung der Datenschutzbehörde über die Ausnahmen von der Datenschutz-Folgenabschätzung (DSFA-AV) und orientiert sich an den „Leitlinien des Europäischen Datenschutzausschusses zur Datenschutz-Folgenabschätzung“, 17/DE WP 248.

Besonderer Teil

Zu § 1:

Hier wird – in Umsetzung der unionsrechtlichen Vorgaben der DSGVO – der Geltungsbereich festgelegt. Eine Datenschutz-Folgenabschätzung ist weiters auch dann durchzuführen, wenn sie zwar nicht durch die gegenständliche Verordnung vorgesehen ist, aber aufgrund des Artikel 35 Abs. 1 oder Abs. 3 DSGVO vorgenommen werden muss. Wird die Verarbeitungstätigkeit eines Verantwortlichen in der vorliegenden Verordnung nicht angeführt, 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 Artikel 35 Abs. 1 erfüllt. Diese Bestimmung ist gemäß Art. 35 Abs. 10 DSGVO nicht anzuwenden, falls die Verarbeitung gemäß Art. 6 Abs. 1 lit. c oder lit. e DSGVO auf einer Rechtsgrundlage im Unions- oder im österreichischen Recht, dem der Verantwortliche unterliegt, beruht und soweit diese Rechtsvorschriften den konkreten Verarbeitungsvorgang, oder die konkreten Verarbeitungsvorgänge regeln und bereits im Rahmen der allgemeinen Folgenabschätzung im Zusammenhang mit dem Erlass dieser Normen eine Datenschutz-Folgenabschätzung erfolgte.

Zu § 2:

Abs. 1:

Abs. 1 legt fest, dass die Datenschutz-Folgenabschätzung nur bei jenen Datenverarbeitungen durchzuführen ist, die rechtmäßig, dh. unter den in Art. 6 DSGVO genannten Bedingungen, erfolgen und sofern nicht eine Ausnahme gemäß DSFA-AV vorliegt.

Abs. 2

Diese Bestimmung enthält den Hinweis, dass ein Verantwortlicher die Datenschutz-Folgenabschätzung durchzuführen hat, sobald ein Vorbereitungsvorgang eines der in den Z 1 bis Z 7 genannten Kriterien erfüllt.

Zu Z 1:

Die betroffene Person sollte das Recht haben, keiner Entscheidung — was eine Maßnahme einschließen kann — zur Bewertung von sie betreffenden persönlichen Aspekten unterworfen zu werden, die ausschließlich auf einer automatisierten Verarbeitung beruht und die rechtliche Wirkung für die betroffene Person entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt, wie die automatische Ablehnung eines Online-Kreditantrags oder Online-Einstellungsverfahren ohne jegliches menschliches Eingreifen. Zu einer derartigen Verarbeitung zählt auch das „Profiling", das in jeglicher Form automatisierter Verarbeitung personenbezogener Daten unter Bewertung der persönlichen Aspekte in Bezug auf eine natürliche Person besteht, insbesondere zur Analyse oder Prognose von Aspekten bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben oder Interessen, Zuverlässigkeit oder Verhalten, Aufenthaltsort oder Ortswechsel der betroffenen Person, soweit dies rechtliche Wirkung für die betroffene Person entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.

Dieses Kriterium umfasst beispielsweise folgende Vorgänge:

a) Verarbeitungsvorgänge im Zusammenhang mit Bonitätsdatenbanken, mit deren Hilfe Betroffenen der Zugriff auf eine Dienstleistung oder der Abschluss eines Vertrages gestattet, geändert oder verwehrt werden soll.
b) Ein Kreditinstitut, das eine von Kreditauskunfteien betriebene Datenbank, eine im Sinne der Verfahren für die Bekämpfung der Geldwäscherei und der Terrorismusbekämpfung eingerichtete Datenbank oder eine Betrugsdatenbank nach seinen Kunden durchsucht.
c) Ein Biotechnologie-Unternehmen, das sich zwecks genetischer Tests direkt an die Betroffenen wendet, um die Erkrankungs- oder Gesundheitsrisiken abzuschätzen bzw. prognostizieren zu können.
d) Ein Unternehmen, das anhand der Nutzung seiner Website bzw. der Navigation der Website durch die Nutzer Verhaltens- oder Marketingprofile (ausgenommen personalisierte Werbung) erstellt.
e) Ein „Dating-Portal" erstellt Profile der Nutzer.

Die Verarbeitung zum Aufenthaltsort oder den Ortswechsel von natürlichen Personen kann beispielsweise durch die gewöhnlichen GPS-Standortbestimmungsdaten aber auch durch Apps erfolgen. Von der Bestimmung sind somit Daten im Sinne des § 92 Abs. 3 Z 6 TKG 2003, aber auch Standort-Daten, die mittels Apps oder Messenger-Dienste erfasst werden können, umfasst.

Zu Z 2:

Profiling und automatisierte Entscheidungsfindung (das heißt, Entscheidungen werden ausschließlich auf technischem Wege, ohne menschliches Eingreifen getroffen) werden in immer mehr Branchen eingesetzt, sowohl im privaten als auch im öffentlichen Bereich. Der Bereich des Banken- und Finanzsektors, Gesundheitswesens, Steuerwesens, der Versicherungen, Marketings und der Werbung sind nur einige Beispiele für die Bereiche, in denen die Profilerstellung regelmäßig durchgeführt wird, um die Entscheidungsfindung zu erleichtern. Da der technologische Fortschritt und die Möglichkeiten neuartiger BIG DATA-Technologien die Gefahr bergen, die Rechte und Freiheiten des Einzelnen erheblich zu beeinträchtigen, ist für diese Kategorie der Datenverarbeitung eine Datenschutz-Folgenabschätzung vorgesehen.

Zu Z 3:

Diese Form der Überwachung insbesondere mittels Bildverarbeitung 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. Darunter fallen beispielsweise Bildverarbeitungen an Örtlichkeiten, die aufgrund eines Kontrahierungszwanges (insbesondere bei Innehabung einer Monopolstellung, dh. wo faktische Übermacht eines Beteiligten ihm die Möglichkeit der „Fremdbestimmung“ über andere gibt, wie beispielsweise bei Verkehrsbetrieben) oder aufgrund eines öffentlichen Interesses von jedermann betreten werden können (wie beispielsweise Spitäler, Ämter und Behörden sowie Polizeidienststellen). Weiters wird damit der Einsatz von sogenannten „Bodycams“ (ausgenommen die Bildverarbeitung erfolgt durch Medienunternehmen oder durch „Blogger“) und die Videoüberwachung zu Überwachungszwecken bei Mehrparteienhäusern samt Garten, Terrasse und Balkon, die nicht ausschließlich vom Nutzungsberechtigten und im gemeinsamen Haushalt Lebenden genutzt werden, umfasst. Ebenso umfasst ist die Überwachung von Stätten, die der Religionsausübung dienen.

Zu Z 4:

Dieses Kriterium umfasst beispielweise die Kombination aus Fingerabdruck- und (biometrischer) Gesichtserkennung zum Zwecke einer verbesserten Zugangskontrolle. Das liegt daran, dass der Einsatz solcher Technologien mit neuartigen Formen der Datenerfassung und -nutzung einhergehen kann, was möglicherweise ein hohes Risiko für die Rechte und Freiheiten von Personen birgt.

Zu Z 5:

Dies betrifft Datenverarbeitungen von gemeinsamen Verantwortlichen iSd Art. 26 DSGVO. Hier ist im Regelfall von einem hohen Risiko auszugehen, weil zwei oder mehr Verantwortliche die Entscheidungsgewalt innehaben und große Datenmengen verarbeitet werden.

Zu Z 6:

Dieses Kriterium umfasst beispielsweise sogenannte „Scoringmethoden“, dh eine Erhebung oder Verwendung von Wahrscheinlichkeitswerten für ein bestimmtes zukünftiges Verhalten eines Betroffenen, um über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses entscheiden zu können und bei denen in einem systematischen Verfahren zum Vergleich und zur Bewertung ein Punktesystem angewendet wird. Weiters umfasst sind sogenannte „Fraud-Prevention-Systeme“, in welchen beispielsweise der Betreiber eines Onlineshops Daten zur Prävention von Betrugsfällen verarbeitet, wobei das Ergebnis der Prüfung ein Risikowert ist, der darüber entscheidet, ob einem Käufer der Rechnungskauf als Zahlungsart angeboten wird oder nicht. Entscheidend ist, dass Daten aus zwei oder mehreren Verarbeitungen „verschnitten“ werden und die Verarbeitung über die vom Betroffenen üblicherweise, dh. nach der Verkehrsauffassung oder den Verkehrssitten bzw. nach der Lebenserfahrung im Regelfall – ohne das Vorliegen außergewöhnlicher Umstände – zu erwartenden Verarbeitungen hinausgeht.

Zu Z 7:

Dieses Kriterium umfasst den höchstpersönlichen Lebensbereich, der den Kernbereich der geschützten Privatsphäre darstellt. Dazu zählen jedenfalls die Gesundheit, das Sexualleben und das Leben in und mit der Familie.

Zu Abs. 3:

Zu Z 1:

Dieses Kriterium umfasst die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung.

Zu Z 2:

Dieses Kriterium umfasst die Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten, einschließlich Verwaltungsübertretungen.

Zu Z 3:

Die Erfassung von Standortdaten im Sinne des TKG 2003 umfasst insbesondere auch die Datenverarbeitung mittels GPS, dh. ein auf Signalen von Satelliten beruhendes, weltweit funktionierendes Hilfsmittel zur exakten Navigation oder Ortsbestimmung.

Zu Z 4:

Die Verarbeitung dieser Art von Daten stellt ein Kriterium dar, weil zwischen den Betroffenen und dem für die Datenverarbeitung Verantwortlichen ein Machtungleichgewicht vorliegt; dh 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 Kinder bis zum vollendeten 14. Lebensjahr (bei ihnen kann nicht davon ausgegangen werden, dass sie in der Lage sind, der Verarbeitung ihrer Daten wissentlich und überlegt zu widersprechen bzw. zuzustimmen), Arbeitnehmer, sowie Teile der Bevölkerung mit besonderem Schutzbedarf wie Patienten, psychisch Kranke und Asylbewerber sowie Betroffene in Situationen, in denen ein ungleiches Verhältnis zwischen der Stellung des Betroffenen und der des Verantwortlichen vorliegt, wie insbesondere Personen, für welche ein Erwachsenenvertreter bestellt wurde. Die Verarbeitung von Arbeitnehmerdaten ist von dieser Bestimmung nur insofern umfasst, als sie nicht bloß zum Zweck der Personalverwaltung erfolgt (vgl. dazu § 2 Abs. 1 des vorliegenden Entwurfes in Verbindung mit der in der Anlage unter DSFA- A02 der DSFA-AV normierten Ausnahme). Die Bestimmung betreffend die Datenverarbeitung von Patienten ist nur anzuwenden, sofern sie nicht bloß von einzelnen Ärzten erfolgt (vgl. dazu § 2 Abs. 1 des vorliegenden Entwurfes in Verbindung mit der in der Anlage unter DSFA-A12 der DSFA-AV normierten Ausnahme).