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), in der Fassung der Berichtigung ABl. Nr. L 127 vom 23.5.2018 S. 2, 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 zu 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.

Der Verordnungsentwurf wurde unter Anwendung des Kohärenzverfahrens im Sinne des Art. 35 Abs. 6 iVm Art. 63 dem Europäischen Datenschutzausschuss (im Folgenden: Ausschuss) übermittelt. Der Stellungnahme des Ausschusses „Stellungnahme 1/2018 zum Entwurf der Liste der zuständigen Aufsichtsbehörde Österreichs in Bezug auf die Verarbeitungen, für die eine Folgenabschätzung zum Datenschutz erforderlich ist (Artikel 35 Absatz 4 DSGVO)“ (siehe dazu unter folgendem Link „Opinion 1/2018 Austrian SAs DPIA List“ https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_en) vom 25.9.2018 wurde Rechnung getragen.

Nach der DSGVO müssen die Verantwortlichen geeignete Maßnahmen ergreifen, um sicherzustellen – und den Nachweis dafür 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 dieser Verordnung 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. Die Verordnung 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 Rev.01.

Für Verarbeitungsvorgänge, die von dieser Verordnung erfasst sind, ist jedenfalls eine Datenschutz-Folgenabschätzung durchzuführen. Dies bedeutet jedoch nicht, dass Verarbeitungsvorgänge, die von dieser Verordnung nicht erfasst sind, keiner Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung unterliegen. Bei Verarbeitungsvorgängen, die weder von dieser Verordnung, noch von der DSFA-AV erfasst sind, ist daher im Einzelfall zu prüfen, ob eine Datenschutz-Folgenabschätzung erforderlich ist oder nicht.

Verarbeitungsvorgänge nach dem 3. Hauptstück des DSG (§§ 36 ff; Verarbeitung personenbezogener Daten für Zwecke der Sicherheitspolizei einschließlich des polizeilichen Staatsschutzes, des militärischen Eigenschutzes, der Aufklärung und Verfolgung von Straftaten, der Strafvollstreckung und des Maßnahmenvollzugs) sind von dieser Verordnung nicht erfasst.

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 Datenschutz-Folgenabschätzung 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 Art. 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:

Zu Abs. 1:

Abs. 1 legt fest, dass die Datenschutz-Folgenabschätzung nur bei jenen Datenverarbeitungen durchgeführt werden kann, die rechtmäßig, dh. unter den in Art. 6, 9 und 10 DSGVO genannten Bedingungen, erfolgen und sofern nicht eine Ausnahme gemäß DSFA-AV vorliegt.

Zu Abs. 2:

Diese Bestimmung enthält den Hinweis, dass ein Verantwortlicher die Datenschutz-Folgenabschätzung durchzuführen hat, sobald zumindest ein Verarbeitungsvorgang eines der in den Z 1 bis Z 6 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 abschätzen 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 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 App oder Messenger-Diensten 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, des Marketings und der Werbung sind nur einige

Beispiele für Bereiche, in denen eine Profilerstellung regelmäßig durchgeführt wird, um die Entscheidungsfindung zu erleichtern. Dabei kann auch auf ein mögliches zukünftiges Verhalten einer betroffenen Person geschlossen werden. 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 wesentliches 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 bspw. Spitäler, Ämter und Behörden sowie Polizeidienststellen). Nicht entscheidend ist, ob die Örtlichkeit erst nach Durchschreiten einer Sicherheitskontrolle betreten werden kann, weil eine Sicherheitskontrolle jedermann in gleicher Weise trifft und den Zutritt aufgrund eines öffentlichen Interesses oder eines Kontrahierungszwanges nicht infrage stellt. Weiters wird damit der Einsatz von sogenannten Körperkameras („Bodycams“; außer, 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 in der Gemeinschaft dienen.

Zu Z 4:

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

Zu Z 5:

Dieses Kriterium umfasst bspw. 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 6:

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. Erfasst werden sollen nicht Datenverarbeitungen, die den höchstpersönlichen Lebensbereich lediglich berühren (wie bspw. das Erfassen von Daten über die Gesundheit während eines Aufnahmegespräches), sondern Datenverarbeitungen, die im höchstpersönlichen Wirkungsbereich erfolgen. Dazu zählen etwa Bildaufnahmen in Sanitäranlagen, Bildaufnahmen von Wohnungsgängen in Mehrparteienhäusern, Datenaufzeichnungen im Rahmen von Selbsthilfegruppen etc. Das hohe Risiko für die Rechte und Freiheiten von Betroffenen lässt sich daraus ableiten, dass selbst im Falle einer Einwilligung für diese Art der Datenverarbeitung, dennoch nicht ausgeschlossen werden kann, dass diese Daten – wenn auch nicht vorsätzlich, sondern bspw. durch bloße Unachtsamkeit – zum Nachteil der betroffenen Personen verwendet werden können, etwa durch Übermittlung.

Verarbeitungsvorgänge, die von der DSFA-AV erfasst sind, fallen nicht unter diese Ziffer.

Zu Abs. 3:

Abs 3 normiert jene Fälle, in denen vom Verantwortlichen eine Datenschutzfolgenabschätzung durchzuführen ist, wenn ein Verarbeitungsvorgang mindestens zwei der Kriterien der Z 1 bis 5 erfüllt.

Zu Z 1 und Z 2:

Z 1 umfasst die umfangreiche 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.

Z 2 umfasst die umfangreiche Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten, einschließlich Verwaltungsübertretungen.

In Z 1 und 2 wird im Einklang mit Art. 35 Abs. 3 lit. b DSGVO auf eine umfangreiche Verarbeitung abgestellt. Der Ausschuss hat in seinen Leitlinien zur Datenschutz-Folgenabschätzung“, 17/DE WP 248 Rev. 01, Seite 11, Faktoren definiert, die für eine umfangreiche Verarbeitung sprechen und empfiehlt deren Berücksichtigung, wenn ermittelt werden soll, ob die fragliche Verarbeitung in großem Umfang durchgeführt wird:

a) Zahl der Betroffenen, entweder als konkrete Anzahl oder als Anteil der entsprechenden Bevölkerungsgruppe;
b) verarbeitete Datenmenge bzw. Bandbreite der unterschiedlichen verarbeiteten Datenelemente;
c) Dauer oder Dauerhaftigkeit der Datenverarbeitung;
d) geografisches Ausmaß der Datenverarbeitung.

Eine ziffernmäßige Festlegung in der Liste nach Art. 35 Abs. 4 DSGVO wird seitens des Ausschusses als nicht erforderlich angesehen (vgl. dazu die Stellungnahme des EDSA Nr. 6/2018 vom 25. September 2018, abrufbar unter https://edpb.europa.eu/sites/edpb/files/files/file1/2018-09-25-opinion_2018_art._64_ee_sas_dpia_list_en.pdf).

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. Der Verweis auf die Definition von Standortdaten nach dem TKG 2003 bedeutet nicht, dass die Adressaten dieser Norm auf jene, welche (nur) dem TKG 2003 unterliegen, eingeschränkt werden.

Zu Z 4:

Die Verarbeitung dieser Art von Daten stellt ein Kriterium dar, weil zwischen den Betroffenen und dem 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 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 in Verbindung mit der in der Anlage unter DSFA-A12 der DSFA-AV normierten Ausnahme). In Bezug auf Arbeitnehmer soll § 2 Abs. 2 letzter Satz sinngemäß gelten, da dies sonst dazu führen könnte, dass eine Datenschutz-Folgenabschätzung bei Vorliegen der Voraussetzungen nach Abs. 2 letzter Satz entfallen könnte, nicht jedoch eine Datenverarbeitung nach Abs. 3 bei Hinzutreten eines weiteren Kriteriums.

Zu Z 5:

Z 5 gleicht im Wesentlichen Abs. 2 Z 5 mit der Maßgabe, dass nicht alle Daten bei der betroffenen Person selbst erhoben wurden. Damit wird der Stellungnahme des Ausschusses Rechnung getragen.