Erläuterungen

Allgemeiner Teil

Hauptgesichtspunkte des Entwurfes:

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 ab 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. 5 DSGVO kann die Aufsichtsbehörde eine Liste der Arten von Verarbeitungsvorgängen erstellen und veröffentlichen, für die keine Datenschutz-Folgenabschätzung erforderlich ist.

Das Datenschutzgesetz (DSG), BGBl. I Nr. 165/1999, tritt – von einigen Ausnahmen abgesehen – 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. 5 DSGVO im Wege einer Verordnung im Bundesgesetzblatt kundzumachen. Nach § 66 DSG dürfen Verordnungen auf Grund des DSG bereits von dem Tag an erlassen werden, der der Kundmachung der durchzuführenden Gesetzesbestimmung folgt; sie dürfen jedoch nicht vor den durchzuführenden Gesetzesbestimmungen in Kraft treten.

Folglich kann die Datenschutzbehörde bereits vor dem 25. Mai 2018 die entsprechende Verordnung erlassen.

An die Datenschutzbehörde wurde vielfach der Wunsch herangetragen, von der Verordnungsermächtigung nach Art. 35 Abs. 5 DSGVO in Verbindung mit § 21 Abs. 2 DSG Gebrauch zu machen. Ziel ist die Auflistung jener Verarbeitungsvorgänge, bei denen vom Vorliegen eines hohen Risikos für die Rechte und Freiheiten natürlicher Personen nicht auszugehen ist und welche folglich der Verpflichtung zur Durchführung einer Datenschutz-Folgenabschätzung nicht unterliegen. Der Entwurf fußt inhaltlich auf der (noch bis zum Ablauf des 24. Mai 2018 in Kraft stehenden) Standard- und Musterverordnung 2004 (StMV), BGBl. II Nr. 312. Ein inhaltliches Aufbauen auf der StMV scheint insofern geboten, als diese Datenanwendungen beinhaltet, bei denen von einer Gefährdung schutzwürdiger Geheimhaltungsinteressen von Betroffenen nicht auszugehen ist. Der Entwurf bereinigt und vereinfacht die Systematik jedoch erheblich.

Gewisse gesetzlich vorgesehene Verarbeitungen, die bereits vor dem 25. Mai 2018 betrieben wurden, sollen von einer Datenschutz-Folgenabschätzung ausgenommen werden. Erfahren solche Verarbeitungen wesentliche Änderungen oder werden neue Verarbeitungen gesetzlich bestimmt, ist zu prüfen, ob eine Datenschutz-Folgenabschätzung erforderlich ist. Art. 35 Abs. 10 DSGVO eröffnet die Möglichkeit, eine Datenschutz-Folgenabschätzung im Rahmen des Gesetzgebungsprozesses durchzuführen.

Die StMV bewirkte, dass die darin genannten Datenanwendungen entweder von der Meldepflicht an die Datenschutzbehörde ausgenommen waren oder einem vereinfachten Melderegime unterlagen. Die Tatsache, dass die Verordnung nach § 21 Abs. 2 DSG inhaltlich an die StMV anknüpft bedeutet jedoch nicht, dass damit – in Analogie zur Wirkung der StMV – eine Befreiung von der Führung eines Verzeichnisses nach Art. 30 DSGVO verbunden wäre. Die Pflicht zur Führung eines derartigen Verzeichnisses besteht unabhängig von der Frage, ob eine Datenschutz-Folgenabschätzung durchzuführen ist oder nicht.

Besonderer Teil

Zu § 1:

Abs. 1 enthält den Hinweis, dass alle in der Anlage angeführten Datenverarbeitungen keiner Datenschutz-Folgenabschätzung im Sinne des Art. 35 Abs. 1 und 5 DSGVO unterliegen. Bei diesen Datenverarbeitungen ist von keinem hohen Risiko für die Rechte und Freiheiten natürlicher Personen auszugehen.

Abs. 1 gilt für alle Verarbeitungen, die nach Ablauf des 24. Mai 2018 vorgenommen werden.

Bei Abs. 2 wird bewusst der Begriff „Datenanwendungen“ im Sinne von § 4 Z 7 des Datenschutzgesetzes 2000 – DSG 2000, BGBl. I Nr. 165/1999 idF BGBl. I Nr. 83/2013, verwendet, weil in Abs. 2 ausdrücklich auf das DSG 2000 Bezug genommen wird.

Abs. 2 Z 1 fußt auf Erwägungsgrund 171 DSGVO, wonach Genehmigungen der Aufsichtsbehörde in Kraft bleiben, bis sie geändert, ersetzt oder aufgehoben werden. Z 1 stellt klar, dass jene Datenanwendungen, die vor dem 25. Mai 2018 nach Durchführung einer Vorabkontrolle von der Datenschutzbehörde im Datenverarbeitungsregister registriert wurden, ebenfalls keiner Datenschutz-Folgenabschätzung unterliegen. Datenanwendungen, die der Vorabkontrolle unterlagen, wurden vor ihrer Registrierung einem Prüfverfahren unterzogen, ob sie mit datenschutzrechtlichen Vorgaben im Einklang stehen. Nur wenn diese Art der Datenverarbeitung zulässig war, erfolgte eine Registrierung im Datenverarbeitungsregister, gegebenenfalls unter Auflagen. War dies nicht der Fall, erfolgte eine (bescheidmäßige) Ablehnung (siehe dazu etwa das Erkenntnis des Verwaltungsgerichtshofes vom 12. September 2016, Zl. Ro 2015/04/0011). Es ist daher angebracht, die im Rahmen einer Vorabkontrolle geprüften Datenanwendungen von einer Datenschutz-Folgenabschätzung auszunehmen, weil die datenschutzkonforme Verarbeitung durch die Registrierung bestätigt wurde, was einer Genehmigung gleichgehalten werden kann (siehe dazu auch die Ausführungen in den von der Gruppe nach Art. 29 der Richtlinie 95/46/EG - Datenschutz-Richtlinie angenommenen „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“, WP 248 Rev.01 vom 4. April 2017).

Erfasst werden sollen auch Datenanwendungen, die in der StMV angeführt und folglich von einer Meldung ausgenommen waren (Z 2). Hier ging der Verordnungsgeber von einem geringen Risiko für die Rechte und Freiheiten natürlicher Personen aus, weshalb es angemessen scheint, auch diese Datenanwendungen von der Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung auszunehmen.

Die Ausnahmen nach Z 1 und 2 treffen zu, wenn diese Datenanwendungen mit Ablauf des 24. Mai 2018 den Vorgaben des DSG 2000 entsprechen und nicht wesentlich geändert werden. Kommt es hingegen zu einer wesentlichen Änderung (bspw. wenn der Überwachungsbereich einer Bildverarbeitung deutlich erweitert wird), ist vom Verantwortlichen zu prüfen, ob eine Datenschutz-Folgenabschätzung durchzuführen ist.

Bei Datenanwendungen, die nach §§ 17 ff DSG 2000 keiner Vorabkontrolle unterlagen und folglich nur automationsunterstützt registriert wurden, kommen die genannten Ausnahmen nicht in Betracht.

Zur Anlage:

Zu DSFA-A01 (Kundenverwaltung, Rechnungswesen, Logistik, Buchführung):

Diese Ausnahme umfasst Verarbeitungstätigkeiten, die in der Mehrzahl der Unternehmen grundsätzlich in standardisierter Form Anwendung finden. Neben der Kundenverwaltung, dem Rechnungswesen, der Logistik und der Buchführung fallen hier insbesondere auch Verarbeitungstätigkeiten wie die Terminverwaltung, die Verwaltung von KursteilnehmerInnen, die Kundenverwaltung und Verrechnung ärztlich verordneter Heilbehelfe und Hilfsmittel durch Gewerbetreibende sowie Bankgeschäfte nach dem Bankwesengesetz.

Festgehalten wird, dass Verarbeitungstätigkeiten von Unternehmen, die Daten über Dritte verarbeiten (keine Kunden des Verantwortlichen), mit denen die Unternehmen in keiner Geschäftsbeziehung stehen, nicht unter diese Ausnahme subsumiert werden können. Es sind dies etwa Detektivbüros, Inkassobüros oder Kreditauskunfteien.

Zu DSFA-A02 (Personalverwaltung für privatrechtliche und öffentlich-rechtliche Dienstverhältnisse):

Diese Ausnahme umfasst Personalverwaltungen sowohl im privaten als auch im öffentlichen Bereich. Darunter fallen neben den vormaligen Standardanwendungen SA002 (Personalverwaltung für privatrechtliche Dienstverhältnisse), SA013 (Personalverwaltung des Bundes und der bundesnahen Rechtsträger) und SA015 (Personalverwaltung der Länder, Gemeinden und Gemeindeverbände) auch SA016 (im Rahmen der Verwaltung von Kammerfunktionären), SA017 (im Rahmen der Verwaltung von Entsendungsdaten der Mitarbeiter) und SA033 (A. Konzernweite Kontakt- und Termindatenbank, B. Karrieredatenbank, C. Verwaltung von Bonus- und Beteiligungsprogrammen eines Konzerns sowie D. Technische Unterstützung).

Zu DSFA-A03 (Mitgliederverwaltung):

Darunter fallen unter anderem die vormaligen Standardanwendungen SA003 (Mitgliederverwaltung), SA016 (im Rahmen der Verwaltung von Kammermitgliedern), SA017 (im Rahmen der Verwaltung von Entsendungsdaten der Mitglieder) und SA018 (im Rahmen der Betreuung von Mitgliedern).

Zu DSFA-A08 (Zutrittskontrollsysteme):

Unter diese Ausnahme wird die Verwaltung von Berechtigungen hinsichtlich des Zutritts zu Objekten bzw. zu bestimmten Bereichen innerhalb von Objekten als auch das Protokollieren der tatsächlich erfolgten Zutritte subsumiert, jedoch nur, solange in diesem Zusammenhang keine biometrischen Daten im Sinne des Art. 4 Z 14 DSGVO verarbeitet werden. Das Verarbeiten von mittels Kameras angefertigten Gesichtsbildern eines Betroffenen ohne Datenaufzeichnung (z.B. im Rahmen der optischen Übertragung von Bilddaten im Rahmen einer Gegensprechanlage) soll hingegen sehr wohl unter diese Ausnahme fallen. Ein automationsunterstützter Abgleich von mittels Bildaufnahmen gewonnenen personenbezogenen Daten mit anderen personenbezogenen Daten fällt hingegen nicht unter diese Ausnahme, zumal ein solcher Abgleich gemäß § 12 Abs. 4 Z 3 DSG ohnehin unzulässig ist.

Zu DSFA-A09 (Stationäre Bildverarbeitung und die damit verbundene Akustikverarbeitung zu Überwachungszwecken (Videoüberwachung)):

Unter Punkt A. dieser Ausnahme fallen Einfamilienhäuser (bzw. die eigene Wohnung) samt Garten, Terrasse oder Balkon. Ebenso umfasst sind die Garage und das Carport auf dem eigenen Grundstück sowie der eigene, gemietete oder gepachtete Parkplatz in einer Gemeinschaftsgarage oder auf einem Gemeinschaftsparkplatz, jeweils unter der Voraussetzung, dass die Einwilligung aller im Einfamilienhaus oder in der Wohnung lebenden Personen zur Videoüberwachung vorliegt, und dass keine fremden Grundstücke/Parkplätze oder unbeteiligte Dritte (Nachbarn oder Passanten) von den Kameras erfasst werden. Ebenso wenig ist die Überwachung des öffentlichen Raums zulässig (außer im unbedingt erforderlichem Ausmaß). Bei einer solchen Überwachung handelt es sich nicht um einen Anwendungsfall der Haushaltsausnahme (vgl. EuGH Urteil vom 11.12.2014, C-212/13 - Ryneš).

Unter Punkt B. dieser Ausnahme fallen Videoüberwachungen im Rahmen der vormaligen Standardanwendungen SA0032 insbesondere im Hinblick auf Banken, Juweliere, Händler mit Antiquitäten und Kunstgegenständen, Gold- und Silberschmiede, Trafiken, Tankstellen oder Parkgaragen und -plätze (auch Parkflächen von Einkaufszentren). Darüber hinaus ist diese Ausnahme vorgesehen für folgende Örtlichkeiten: allgemein zugängliche Bereiche der Geschäftsräumlichkeiten und des Betriebsgeländes von Unternehmen, welche nicht der Betriebsratspflicht unterliegen; sämtliche Bereiche der Geschäftsräumlichkeiten und des Betriebsgeländes von Unternehmen mit Betriebsratspflicht, sofern eine gültige Betriebsvereinbarung über die gegenständliche Videoüberwachung existiert und diese Räumlichkeiten von der Betriebsvereinbarung umfasst sind; öffentliche Verwaltungsgebäude mit gültiger Zustimmung der Personalvertretung; Vereinsräumlichkeiten; Sportstätten; Freizeiteinrichtungen; Kultureinrichtungen oder dergleichen.

Keine Anwendung findet diese Ausnahme auf Örtlichkeiten, welche aufgrund eines bestehenden Kontrahierungszwanges oder aufgrund des öffentlichen Interesses von jedermann betreten werden dürfen (Verkehrseinrichtungen, Spitäler etc.) trotz Vorliegens einer Betriebsvereinbarung oder einer Zustimmung der Personalvertretung. Diese Ausnahme trifft auch nicht auf mobile Kameras (insbesondere Bodycams) zu.

In allen Fällen ist jedenfalls der Verhältnismäßigkeitsgrundsatz einzuhalten.

Zum räumlichen Erfassungsbereich:

Nach ständiger Rechtsprechung der Datenschutzbehörde können Verantwortliche des privaten Bereichs (zB Firmen, Vereine, natürliche Personen) sowie Verantwortliche des öffentlichen Bereichs im Rahmen der Privatwirtschaftsverwaltung ein „berechtigtes Interesse“ an einer Videoüberwachung (im Sinne einer systematischen Kontrolle eines Raumes) allenfalls aus dem Bestehen eines Hausrechts ableiten. Private dürfen somit prinzipiell nur dort Videoüberwachung betreiben, wo das Bestehen oder der Schutz eines „Hausrechts im weiteren Sinn“ denkbar ist, also jedenfalls nicht an öffentlichen Orten („öffentlicher Raum“). Würde eine Videoüberwachung durch einen Privaten (in einem erheblichen Ausmaß) auch öffentlichen Raum erfassen, so wäre diese - egal zu welchem Zweck - grundsätzlich unzulässig. Unter Umständen wäre es jedoch aufgrund von erfolgten Sachbeschädigungen oder Gefährdungen denkbar, die Fassade eines Gebäudes/den Zaun eines Grundstückes unter größtmöglicher Schonung unbeteiligter Dritter mittels einer Videoanlage zu überwachen. Hierfür müsste allerdings der jeweilige Kamerawinkel so gewählt werden, dass höchstens der unmittelbar an das Grundstück angrenzende Teil des Gehsteiges im notwendigen Ausmaß (maximal ca. 50 cm) auf dem Bildmaterial zu erkennen ist, nicht jedoch der gesamte Gehsteig, Parkplätze oder Teile der Fahrbahn.

Zur Speicherdauer:

Gemäß § 13 Abs. 3 DSG sind aufgenommene personenbezogene Daten vom Verantwortlichen zu löschen, wenn sie für den Zweck, für den sie ermittelt wurden, nicht mehr benötigt werden und keine andere gesetzlich vorgesehene Aufbewahrungspflicht besteht. Die gegenständliche Ausnahme umfasst nur Videoüberwachungen mit einer maximalen Speicherdauer von 72 Stunden, es sei denn, eine längere Aufbewahrungsdauer wurde in einem Gesetz, durch einen behördlichen Rechtsakt, in einer Betriebsvereinbarung oder mit Zustimmung der Personalvertretung ausdrücklich festgelegt. Wenn ein Verantwortlicher eine längere Speicherdauer als 72 Stunden vorsehen will und keine der sonstigen in dieser Ausnahme angeführten Voraussetzungen für eine verlängerte Speicherdauer vorliegen, findet die DSFA-A09 keine Anwendung.

Zur Kennzeichnung:

Voraussetzung für diese Ausnahme ist das Vorhandensein einer geeigneten Kennzeichnung der Bild- und gegebenenfalls auch der damit verbundenen Tonverarbeitung im Sinne des § 13 Abs. 5 DSG. Fälle von verdeckten Ermittlungen (vgl. § 13 Abs. 6 DSG) werden von dieser Ausnahme hingegen nie erfasst.

Zu DSFA-A10 (Bild- und Akustikdatenverarbeitung in Echtzeit):

Unter diese Ausnahme fallen Bild- und damit verbundene Akustikdatenverarbeitungen in Echtzeit. Damit sind Kameraanwendungen gemeint, welche die Bilddaten (eventuell verbunden mit Tondaten) ausschließlich live übertragen. Solche Anwendungen unterlagen vor dem In-Geltung-Treten der DSGVO nicht der Meldepflicht gemäß §§ 17 ff des Datenschutzgesetzes (DSG), BGBl. I Nr. 165/1999 idF BGBl. I Nr. 83/2013. Für Echtzeit-Videoüberwachungen galt die Spezialbestimmung des § 50c Abs. 2 Z 1 DSG 2000.

Voraussetzung für diese Ausnahme ist die Verfügungsbefugnis des Verantwortlichen über jene Bereiche, auf welche die Bild- und Tonübertragungsgeräte gerichtet sind sowie das Vorhandensein der geeigneten Kennzeichnung der Bild- und gegebenenfalls auch der Tonverarbeitung im Sinne des § 13 Abs. 5 DSG. Fälle von verdeckten Ermittlungen (vgl. § 13 Abs. 6 DSG) werden von dieser Ausnahme hingegen nicht erfasst. Ebenso wenig sind Bild- und Akustikdatenverarbeitungen, die an Orten betrieben werden, welche den höchstpersönlichen Lebensbereich von Personen darstellen, unter diese Ausnahme subsumierbar, unabhängig davon ob eine ausdrückliche Zustimmung eines Betroffenen vorliegt oder nicht.

Zu DSFA-A11 (Bild- und Akustikverarbeitungen zu Dokumentationszwecken):

Unter diese Ausnahme fallen insbesondere Kameraanwendungen zur Dokumentation des Tierbestandes, zur Beobachtung von Flussläufen, Zeitrafferkameras zur Dokumentation des Baustellenfortschritts etc. Jegliche Auswertung und Weitergabe der Daten über den angegebenen Zweck hinaus (etwa zur Identifizierung von Personen oder Verwendung zum Zweck der Rechtsverfolgung) ist von dieser Ausnahme nicht erfasst.

Voraussetzung für diese Ausnahme ist die Verfügungsbefugnis des Verantwortlichen über jene Bereiche, auf welche die Aufnahmegeräte gerichtet sind. Ebenso das Vorhandensein der geeigneten Kennzeichnung der Bild- und gegebenenfalls auch der Tonverarbeitung im Sinne des § 13 Abs. 5 DSG, es sei denn, die Aufnahmen dienen einem rein privaten Dokumentationsinteresse (vgl. § 13 Abs. 6 iVm § 12 Abs. 3 Z 3 DSG).

Gemäß Art. 2 Abs. 2 lit. c DSGVO findet die DSGVO keine Anwendung auf die Verarbeitung personenbezogener Daten durch natürliche Personen zur Ausübung ausschließlich persönlicher und familiärer Tätigkeiten. Somit unterliegen etwa Urlaubsfotos oder Fotos von Geburtstagsfeiern nicht der Notwenigkeit einer Datenschutz-Folgenabschätzung.

Zu DSFA-A12 (Patienten-/Klienten-/Kundenverwaltung und Honorarabrechnung einzelner Ärzte, Gesundheitsdiensteanbieter und Apotheker):

Laut Erwägungsgrund 91 zur DSGVO gilt eine Verarbeitung von Patientendaten dann nicht als umfangreich, wenn sie durch einen einzelnen Arzt oder sonstigen Angehörigen eines Gesundheitsberufes erfolgt. In diesen Fällen ist eine Datenschutz-Folgenabschätzung nicht zwingend vorgeschrieben.

Die gegenständliche Ausnahme trifft somit im Umkehrschluss nicht auf die Patientenverwaltung bzw. Honorarabrechnung von Krankenhäusern, Ärztezentren, Gemeinschaftspraxen, Gesundheitsinstituten, Kuranstalten etc. zu, da in diesen Fällen besondere Kategorien von Daten im Sinne des Art. 9 DSGVO (Gesundheitsdaten) von schutzbedürftigen Betroffenen in großem Umfang verarbeitet werden.

Zu DSFA-A13 (Rechts- und Beratungsberufe):

Laut Erwägungsgrund 91 zur DSGVO gilt eine Verarbeitung von Daten von Mandanten dann nicht als umfangreich, wenn sie durch einen einzelnen Rechtsanwalt erfolgt. In diesen Fällen ist eine Datenschutz-Folgenabschätzung nicht zwingend vorgeschrieben.

Die Unternehmensberatung einschließlich der Unternehmensorganisation fällt unter die Gewerbeordnung (vgl. § 136 GewO 1994) Da Unternehmensberater unter anderem auch zur berufsmäßigen Vertretung ihrer Auftraggeber gegenüber Dritten, wie insbesondere Kunden und Lieferanten, sowie vor Behörden und Körperschaften öffentlichen Rechts berechtigt sind, fallen sie ebenfalls unter diese Ausnahme

Zu DSFA-A14 (Wissenschaftliche Forschung und Statistik):

Unter diese Ausnahme fallen Verarbeitungstätigkeiten im Zusammenhang mit Archivzwecken, wissenschaftlichen oder historischen Forschungszwecken oder statistischen Zwecken, für die aufgrund des Vorliegens der Voraussetzungen des § 7 Abs. 2 Z 1 und 2 DSG keine Genehmigung der Datenschutzbehörde im Sinne des § 7 Abs. 3 DSG erforderlich ist.

Zu DSFA-A20 (Aktenverwaltung (Büroautomation) und Verfahrensführung):

Unter diese Ausnahme werden ausschließlich Kanzleiprotokollierungssysteme bzw. Aktenverwaltungssysteme (wie etwa der ELAK des Bundes) subsumiert, welche der formellen Verfahrensführung (Protokollierung, Fristenverwaltung, Aktenauffindung, Abfertigung etc.) dienen, nicht jedoch Verarbeitungstätigkeiten, welche zwar in einem Aktenverwaltungssystem erfasst, bearbeitet oder gespeichert werden, jedoch materiellen Akteninhalt darstellen. Dazuzuzählen sind auch elektronische Instrumente der Kommunikation (wie etwa E-Mail-Programme).

Zu DSFA-A21 (Organisation von Veranstaltungen):

Diese Ausnahme umfasst die Organisation von Veranstaltungen aller Art, wie Kongresse, Konferenzen oder Messen.