

Der Entwurf sieht vier Beschränkungen des Grundrechts vor. Art 6 Abs. 1 DSGVO führt allerdings insgesamt sechs Möglichkeiten der Rechtmäßigkeit der Verarbeitung an. Im Entwurf fehlen die Gründe „Erfüllung eines Vertrages“ gemäß Art 6 Abs. 1 lit b DSGVO und „Erfüllung einer rechtlichen Verpflichtung, der der Verantwortliche unterliegt“ gemäß Art 6 Abs. 1 lit c DSGVO. Diese sollten ergänzt werden.

§ 1 Abs. 2 ist daher zu ändern wie folgt:

(2) Beschränkungen sind nur mit Einwilligung der betroffenen Person oder in lebenswichtigem Interesse der betroffenen Person oder in Erfüllung eines Vertrages oder in Erfüllung einer rechtlichen Verpflichtung, der der Verantwortliche unterliegt oder im öffentlichen Interesse und zwar nur aufgrund einer gesetzlichen Grundlage oder im überwiegenden berechtigten Interesse eines anderen zulässig. Diese Beschränkungen müssen notwendig und verhältnismäßig und, insbesondere im Hinblick auf den Zweck, die verarbeiteten Daten und die Art der Verarbeitung für die betroffene Person vorhersehbar sein. Im Rahmen hoheitlicher Tätigkeiten dürfen Beschränkungen nur aufgrund von Gesetzen, die aus den in Art 8 Abs. 2 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK), BGBl. Nr. 210/1958, genannten Gründen notwendig sind, vorgesehen werden.

Zu § 10 Aufgaben, Datenschutzfolgenabschätzung (Art. 35 DSGVO)

Die Datenschutzbehörde hat eine Liste der Verarbeitungsarten zu erstellen und zu führen, für die gemäß Art 35 Abs. 4 DSGVO eine Datenschutz-Folgeabschätzung durchzuführen ist. Wir begrüßen, dass diese Liste im Wege einer Verordnung kundzumachen ist. Begrüßt wird die in § 10 Abs. 2 2018 normierte Verordnungsermächtigung der Datenschutzbehörde zum Erlass der Listen gemäß Art. 35 Abs. 4 und 5 DSGVO zur Festlegung, bei welchen konkreten Datenverarbeitungsvorgängen eine Datenschutzfolgenabschätzung notwendig ist oder nicht. Diese Listen sind für die korrekte Umsetzung der DSGVO von enormer Bedeutung, weswegen die Kundmachung des Datenschutz-Anpassungsgesetzes 2018 und in weiterer Folge der Erlass der oben erwähnten Verordnungen der Datenschutzbehörde so rasch als möglich erfolgen sollten, damit diese Verordnungen noch vor Mai 2018 Berücksichtigung finden können.

Weiters sollte aus unserer Sicht der nationale Gesetzgeber von der Öffnungsklausel gem. Art. 35 Abs. 10 DSGVO Gebrauch machen und zwar dahingehend, dass eine Datenschutzfolgenabschätzung für Verarbeitungstätigkeiten nicht erforderlich ist, die nach Art. 6 Abs. 1 lit c) zur Erfüllung einer rechtlichen Verpflichtung erforderlich sind. Konkretes Beispiel wäre hier die Verarbeitungstätigkeit im Zusammenhang mit Smart-Meter-Anwendungen.

Zu § 11 Befugnisse

Die Übernahme der Bestimmungen aus § 30 DSG 2000, die die Befugnisse der Datenschutzbehörde regeln, wird als sinnvoll erachtet. Allerdings ist nicht zuletzt aufgrund der bestandsgefährdenden Höhe der Strafen die Konkretisierung der Befugnisse, insbesondere im Hinblick auf Einsichts- und Betretungsrechte der Datenschutzbehörde aus Gründen der

Rechtssicherheit, notwendig. Unter welchen Voraussetzungen die Datenschutzbehörde Räumlichkeiten betreten darf bzw. wann eine entsprechende Verständigung des Verantwortlichen hierzu zu erfolgen hat, sollte klar geregelt sein. Die vorliegende Formulierung des **Einschau- und Betretungsrechts der Datenschutzbehörde ist überschießend geregelt:** Gemäß dieser Bestimmung soll die Datenschutzbehörde nicht nur berechtigt sein, die Räume, in welchen Datenverarbeitungen vorgenommen werden, zu betreten. Darüber hinaus soll die Datenschutzbehörde auch befugt werden, „*Datenverarbeitungsanlagen in Betrieb zu setzen*“ sowie „*die zu überprüfenden Verarbeitungen durchzuführen*“. In den Erläuterungen zu dieser Bestimmung heißt es, dass dies eine Umsetzung des Einschau- und Betretungsrechts von Art. 58 Datenschutz-Grundverordnung sei. Tatsächlich sieht diese EU-rechtliche Regelung aber nur vor, dass die Datenschutzbehörde Zugang zu den Geschäftsräumlichkeiten und den Datenverarbeitungsanlagen haben muss. Eine eigenständige Inbetriebsetzung von Anlagen und Durchführung von Verarbeitungen ist darin jedoch nicht geregelt. **Dass die Datenschutzbehörde Anlagen in Betrieb setzen kann und Verarbeitungen an diesen Anlagen selbst durchführen kann, ist demnach weder EU-rechtlich gefordert noch sachlich gerechtfertigt:** Zum einen möchten wir darauf hinweisen, dass eine solche Inbetriebsetzung durch eine Behörde gerade bei kritischer Infrastruktur aus Sicherheitsgründen bedenklich ist. Außerdem ist eine solche Inbetriebsetzung auch nicht notwendig. Es ist mehr als ausreichend, wenn die Verarbeitungsschritte durch den Verpflichteten durchgeführt werden und die Datenschutzbehörde dabei ein Einsichtsrecht hat. Gegebenenfalls kann der Datenschutzbehörde auch ein Protokoll ausgehändigt werden. Aus all diesen Gründen ist die vorgeschlagene Bestimmung nicht verhältnismäßig.

Wir schlagen daher folgende Formulierung von § 11 Abs. 2 Datenschutz-Anpassungsgesetz vor:

„(2) Zum Zweck der Einschau ist die Datenschutzbehörde nach Verständigung des Inhabers der Räumlichkeiten und des Verantwortlichen oder des Auftragsverarbeiters berechtigt, Räume, in welchen Datenverarbeitungen vorgenommen werden, zu betreten und zu veranlassen, dass durch den Datenverarbeiter Datenverarbeitungsanlagen in Betrieb zu gesetzt werden, die zu überprüfenden Verarbeitungen durchzuführen durchgeführt werden sowie Kopien von Datenträgern in dem für die Ausübung der Kontrollbefugnisse unbedingt erforderlichen Ausmaß ~~herzustellen~~ hergestellt werden.“

Zu § 12 Veröffentlichung von Entscheidungen

Zu § 12 Abs. 2

Zur Steigerung der Rechtssicherheit und Orientierung in all den sich aus der DSGVO ergebenden Verpflichtungen und Rechten schlagen wir eine Änderung des § 12 Abs. 2 vor, wonach lediglich „Entscheidungen der Datenschutzbehörde von grundsätzlicher Bedeutung für die Allgemeinheit“ in geeigneter Weise zu veröffentlichen sind. Unter Gewährleistung entsprechender Anonymisierungen plädieren wir für eine Veröffentlichung (von zumindest Kurzsprüchen) aller Entscheidungen der Datenschutzbehörde.

Zu § 15 Verantwortliche des öffentlichen und privaten Bereichs

Zu § 15 Abs. 2

Die Einschränkung auf „*Verantwortliche des öffentlichen Bereichs*“ als „Partei in Verfahren vor der Datenschutzbehörde“ sollte unserer Ansicht nach jedenfalls aufgehoben werden.

Zu § 19 Allgemeine Bedingungen für die Verhängung von Geldbußen

Zu § 19 Abs.3

Die Möglichkeit der Bestrafung eines Verantwortlichen gemäß § 9 VStG in § 19 Abs. 3 entspricht nicht der Zielrichtung der DSGVO, die nur das Unternehmen strafen will. Eine Erweiterung auf verantwortliche Organe bzw. Beauftragte wäre nicht zuletzt aufgrund der Höhe der Geldbußen überschießend. **Wir schlagen daher vor, analog zum Kartellrecht die Strafen auf die Unternehmen zu beschränken und somit § 19 Abs. 3 zu streichen.**

Laut Erläuterungen orientiert sich der Wortlaut des Abs. 3 an § 99d des Bankwesengesetzes (BWG). Die Verantwortlichkeit nach dem BWG wird allerdings in weiteren Bestimmungen dieses Gesetzes klar umschrieben, sodass die isolierte Übertragung des § 99d BWG in den Entwurf darüber hinaus zu einem systemwidrigen Ergebnis führt.

Abschließend sei auf das kürzlich erlassene und am 01.07.2017 in Kraft tretende Deregulierungsgrundsatzgesetz verwiesen, das verhindern soll, dass Rechtsakte der Europäischen Union ohne Grund übererfüllt werden (§ 1 Abs. 4 leg. cit).

Die zusätzliche Strafbarkeit natürlicher Personen ist daher abzulehnen und Abs. 3 ersatzlos zu streichen.

Weiters schlagen wir vor, dass im Datenschutz-Anpassungsgesetz 2018 näher auf die Haftung des Datenschutzbeauftragten eingegangen wird, insbesondere hinsichtlich § 9 VStG. Die Abgrenzung zwischen Datenschutzbeauftragten und § 9 VStG Verantwortlichen sollte geschärft werden, dies vor allem hinsichtlich der Strafbestimmungen und so festgehalten werden, dass der Datenschutzbeauftragte nicht den Strafbestimmungen der DSGVO unterliegt. Auch die Tatsache, dass beide Beauftragungen miteinander – in einer Person – unvereinbar sind, sollte klarer formuliert werden.

Zu § 19 Abs. 5

Vorgesehen ist, dass gegen Behörden und öffentliche Stellen keine Geldbußen verhängt werden können. Das ist jedenfalls kritisch zu betrachten, da das schützenswerte Gut der Schutz der personenbezogenen Daten von Einzelpersonen ist. Mit der vom innerstaatlichen Gesetzgeber vorgenommenen Wertung signalisiert dieser, dass Verletzungen von Seiten der öffentlichen Hand weniger schwer wiegen und offensichtlich nicht einmal ein Bagatelldelikt darstellen. Aus unserer Sicht ist dies ein falsches Signal und daher abzulehnen, noch dazu vor dem Hintergrund, dass die öffentliche Hand über Zugang zu ganz wesentlichen, oftmals auch sensiblen, personenbezogenen Daten verfügt.

§ 29 Verarbeitung personenbezogener Daten im Beschäftigungskontext

§ 29 Datenschutz-Anpassungsgesetz regelt, dass das Arbeitsverfassungsgesetz (ArbVG) eine Vorschrift im Sinne des Art 88 DSGVO ist. Unklar ist, ob das ArbVG somit direkt dem Haftungsregime der DSGVO unterliegt. Die Notifikation bei der EU-Kommission könnte möglicherweise bedeuten, dass die Strafbestimmungen der DSGVO von Euro 20 Mio oder 4 % vom Umsatz, beispielsweise auch bei Nichtabschluss einer Betriebsvereinbarung zur Arbeitnehmerdatenverarbeitung, anzuwenden sind. Wünschenswert ist daher eine Klarstellung, dass entweder das Strafregime des ArbVG weiterhin Anwendung findet, oder der Strafrahmen gemäß des § 69 Abs. 1 Datenschutz- Anpassungsgesetz in Höhe von maximal Euro 50.000,- Geltung erlangt.

Zu § 30 Zulässigkeit der Bildaufnahme

Mit der neuen Regelung zur Bildverarbeitung werden jegliche Bildaufnahmen umfasst, d.h. nicht nur Video-, sondern auch Fotoaufnahmen, was definitiv überschießend erscheint. Es sollte jedenfalls auf den Zweck der Bildaufnahme abgestellt werden. Ein Eingriff in Rechte von Betroffenen ist mit Sicherheit als schwerwiegender anzusehen, wenn eine systematische Überwachung erfolgt als bei rein privaten Aufnahmen ohne einen Überwachungszweck. Der neue Abs. 3 Z. 3 erscheint nicht ausreichend, um zulässige Privataufnahmen zu machen. Dies vor allem in Zusammenschau mit Abs. 4, der besagt, dass Bildaufnahmen ohne ausdrückliche Einwilligung der betroffenen Person in deren höchstpersönlichen Lebensbereich immer unzulässig sind. Abgesehen vom Kernbereich der Privatsphäre soll auch ein Eingriff in deren Vorfeld unzulässig sein, wie etwa die Kontrolle von Zugängen zu Sakralgebäuden. Dies ist verständlich, wenn es um eine Überwachung bzw., wie auch in den Erläuterungen festgehalten, um die Kontrolle von solchen Zugängen geht. Da aber der Gesetzestext keinen Unterschied zwischen einer Überwachung/Kontrolle und bloßen privaten Aufnahmen ohne einen Überwachungszweck macht, hätte diese Regelung zur Folge, dass alle Bildaufnahmen u. ä. – ob ein privates Dokumentationsinteresse besteht oder nicht – rechtswidrig wären. Es sollte daher jedenfalls eine Differenzierung zwischen Bildaufnahmen zu Überwachungszwecken und Privataufnahmen ohne diesen Zweck erfolgen.

§ 32 Abs. 3 Bildverarbeitung – Besondere Datensicherheitsmaßnahmen – Löschfristen

Gem. § 32 Abs. 3 des Entwurfes zum Datenschutzgesetz DSG sind vom Verantwortlichen die aufgenommenen personenbezogenen Daten zu löschen, wenn sie für den Zweck, für den Sie ermittelt wurden, nicht mehr benötigt werden und keine andere gesetzlich vorgesehene Aufbewahrungspflicht besteht. Zur Klarstellung ist auf die Regelung des § 3 des vorliegenden Entwurfs zu verweisen, wonach die Löschung der personenbezogenen Daten nicht unverzüglich zu erfolgen hat, wenn die Löschung aus wirtschaftlichen und technischen Gründen nur zu bestimmten Zeitpunkten vorgenommen werden kann und die Verarbeitung dieser personenbezogenen Daten bis zu diesem Zeitpunkt einzuschränken ist.

§ 35 Begriffsbestimmungen

In den Begriffsdefinitionen findet sich unter § 35 Z 14 (Gesundheitsdaten) die Definition „*personenbezogener Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person beziehen (...) und aus denen Informationen über deren Gesundheitszustand hervorgehen*“. Gemäß § 39 handelt es sich bei diesen Daten um besondere Kategorien personenbezogener Daten, deren Verarbeitung nur zulässig ist, wenn die Verarbeitung unbedingt erforderlich ist und wirksame Maßnahmen zum Schutz der Rechte und Freiheiten der betroffenen Personen getroffen werden und Punkt 1 sowie 2 erfüllt sind. Hier wäre in den Erläuterungen klarzustellen, dass die Sozialversicherungsnummer (z.B. eines Arbeitnehmers) kein „*Gesundheitsdatum*“ i.S.d. Begriffsdefinition ist.

Zu § 69 Verwaltungsstrafbestimmung

In § 69 Abs. 1 werden die Verwaltungsstrafen, ohne dass die EU-Vorgaben dies verlangen würden, im Verhältnis zum Status quo verdoppelt. Eine derartig drastische Anhebung ist sachlich nicht begründet und wird daher abgelehnt.

Grundsätzlich sind Verwaltungsstrafatbestände, die über die DSGVO hinausgehen, abzulehnen. Bei der Strafbestimmung des § 69 handelt es sich um eine solche. Es ist festzuhalten, dass im entsprechenden Artikel 83 DSGVO keine Öffnungsklausel für diesen Straftatbestand vorgesehen ist. Daher ist zu überlegen, ob nicht nur keine Verdoppelung sondern die gänzliche Streichung des § 69 die systematisch richtige Variante darstellt.

Zu § 76 Übergangs- und Schlussbestimmungen

Bestehende Einwilligungen

Im Erwägungsgrund 171 der DSGVO ist angeführt, dass bereits erteilte Einwilligungen weiterhin Gültigkeit haben sollen, wenn die Einwilligungen den Bedingungen der DSGVO entsprechen. Diese Erwägungsgründe sind jedoch nach der EuGH-Judikatur nicht rechtsverbindlich (siehe EuGH, C-162/97, Nilson, Rn 54) und daher kann der innerstaatliche Gesetzgeber unserer Meinung nach auch Übergangsregelungen definieren, wie es auch der deutsche Gesetzgeber im Entwurf des neuen Bundesdatenschutzgesetzes getan hat. Vor diesem Hintergrund wird eine Regelung im Datenschutz-Anpassungsgesetz 2018 vorgeschlagen, die besagt, dass datenschutzrechtliche Einwilligungen, die vor der Geltung der DSGVO ab Mai 2018 rechtsgültig nach den bis dahin geltenden Datenschutzgesetzen eingeholt wurden, auch weiterhin Gültigkeit haben. Dies sollte insbesondere auch gültige datenschutzrechtliche Einwilligungen, die in Allgemeinen Geschäftsbedingungen eingeholt wurden, betreffen. Ansonsten müsste von Bestandskunden nachträglich eine erneute Zustimmung eingeholt werden, was unnötigen Aufwand für Kunden und Unternehmen bedeuten würde.

Zu § 76 Abs. 4 und 5

Zum Zeitpunkt des Inkrafttretens dieses Bundesgesetzes bei der Datenschutzbehörde oder bei den ordentlichen Gerichten zum DSGVO 2000 anhängige Verfahren sollen laut dem Gesetzestext nach der neuen Rechtslage beurteilt werden. Dies ist unseres Erachtens nach jedenfalls kritisch zu betrachten, da unter Umständen Handlungen, die vor Inkrafttreten dieses Bundesgesetzes bzw. der DSGVO noch keine Verletzungen dargestellt haben, dann plötzlich zu zusätzlichen Straftatbeständen werden könnten.

Weiters wird in den Erläuterungen festgehalten, dass Verletzungen gegen das DSGVO 2000, die vor dem Inkrafttreten dieses Bundesgesetzes noch nicht anhängig gemacht wurden, nach jener Rechtslage zu beurteilen sind, die für den Täter in Ihrer Gesamtauswirkung günstiger ist. Dies findet sich allerdings im Gesetzestext nicht wieder. Eine Klarstellung bzw. Aufnahme im Gesetzestext sollte daher erfolgen.

Schließlich möchten wir noch auf einen redaktionellen Fehler hinweisen: Im letzten Satz von § 26 Abs. 4 des Entwurfes fehlt vor dem Begriff „knüpfen“ das Wort „zu“.

B. Datenschutz-Grundverordnung

Art 6 – Berechtigtes Interesse an einer Datenverarbeitung (Art. 6 Abs. 1 lit f) DSGVO)

Gemäß Art. 6 Abs. 1 lit f) DSGVO ist eine Verarbeitung auch rechtmäßig, wenn diese zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen. Dieses berechtigte Interesse wird im Erwägungsgrund 47 bzw. 48 der DSGVO auch hinsichtlich Direktwerbung und für Verantwortliche, die Teil einer Unternehmensgruppe sind, konkretisiert.

Insbesondere für Konzerngesellschaften ist dieser Rechtsgrund zur Datenverarbeitung wesentlich, sodass eine nähere Ausgestaltung und Konkretisierung im Datenschutz-Anpassungsgesetz 2018 aus unserer Sicht wünschenswert wäre, soweit es die DSGVO zulässt.

Art 8 DSGVO Bedingungen für die Einwilligung eines Kindes

Artikel 8 der DSGVO definiert generell, dass bei einem Angebot von Diensten der Informationsgesellschaft, das einem Kind direkt gemacht wird, die Verarbeitung der personenbezogenen Daten des Kindes rechtmäßig ist, wenn das Kind das sechzehnte Lebensjahr vollendet hat.

Weiters ist in Artikel 8 der DSGVO normiert, dass die Mitgliedstaaten durch Rechtsvorschriften diesbezüglich eine niedrigere Altersgrenze vorsehen können, die jedoch nicht unter dem vollendeten dreizehnten Lebensjahr liegen darf.

