INDUSTRIELLEN VEREINIGUNG
Finanzpolitik & Recht

Schwarzenbergplatz 4, 1031 Wien
Österreich
T: +43 1 711 35-2341
Fax: +43 1 711 35-2923
rp@iv.at
www.iv.at

An das
Bundeskanzleramt-Verfassungsdienst
Ballhausplatz 2
1010 Wien

Per email: v@bka.gv.at
begutachtungsverfahren@parlament.gv.at

Wien, am 23. Juni 2017
M. Ritschl

IV Stellungnahme zum Entwurf eines Bundesgesetzes, mit dem das Bundes-Verfassungsgesetz geändert, das Datenschutzgesetz erlassen und das Datenschutzgesetz 2000 aufgehoben wird (Datenschutz-Anpassungsgesetz 2018)

GZ: BKA-810.026/0019-V/3/2017

Sehr geehrte Damen und Herren,

die Industriellenvereinigung (IV) bedankt sich für die Möglichkeit zur Abgabe einer Stellungnahme zum vorliegenden Entwurf des Datenschutz-Anpassungsgesetzes 2018 und führt wie folgt aus:

I. Allgemeine Anmerkungen

Der vorliegende Entwurf ist aus Sicht der Industrie im Wesentlichen zu begrüßen, da er eine gute Balance zwischen effizientem Datenschutz und notwendiger Rechtssicherheit für die Wirtschaft herstellt. Dass der österreichische Gesetzgeber die Öffnungsklauseln der Datenschutz-Grundverordnung (DSGVO) nur sehr restriktiv genützt hat, ist sowohl aus Sicht des Wetterwerbsstandortes Österreich als auch aus Gründen der Harmonisierung sinnvoll.

Sowohl die DSGVO als auch das österreichische Anpassungsgesetz stellen die Unternehmen in Österreich allerdings aufgrund der vielen Neuerungen und des enormen Strafrahmens vor wesentliche Herausforderungen. Der Zeitdruck zur Implementierung der bis dahin geforderten Maßnahmen ist immens. Um den Unternehmen eine angemessene Vorlaufzeit für die rechtzeitige Implementierung der neuen datenschutzrechtlichen Bestimmungen zu ermöglichen, ist daher eine zeitnahe Beschlussfassung des Gesetzes dringend erforderlich.

Davon unabhängig, weist der gegenständliche Entwurf noch einige Punkte auf, die zum Ziele der Rechtssicherheit, Effizienz und Handhabbarkeit nachgebessert werden sollten. Im Folgenden geht die IV auf die einzelnen Bestimmungen im Detail ein.

II. Anmerkungen im Detail

A. Zu § 1 (Grundrecht auf Datenschutz)

Die Regelung des Grundrechts auf Datenschutz nach § 1 ist in vielen Bereichen strenger als die Vorgaben der DSGVO:

Die Gründe für eine zulässige Beschränkung des Grundrechts auf Datenschutz in Abs 2 sind enger als diejenigen für die Rechtmäßigkeit der Datenverarbeitung in Art 6 Abs 1 DSGVO. Es sollten daher aus Sicht der IV die aus Art 6 Abs 1 DSGVO **fehlenden Rechtmäßigkeitsgründe der „Erfüllung eines Vertrags" (lit b) und die „Erfüllung rechtlicher Verpflichtungen" (lit c) in § 1 Abs 2 aufgenommen werden.**

Des Weiteren sieht § 1 Abs 2 vor, dass Beschränkungen des Grundrechts auf Datenschutz ua nur im „überwiegenden berechtigten Interesse" eines anderen zulässig sind. Hier befände sich die Beweislast demnach beim Verantwortlichen bzw. Auftragsverarbeiter. Dies würde jedoch der DSGVO widersprechen, die bewusst die Beweislast hin zur betroffenen Person verlagert, da sie in Art 6 eine Rechtmäßigkeit der Verarbeitung folgendermaßen normiert: *„zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich (sind), sofern nicht die Interessen … der betroffenen Person… überwiegen".* **Das Wort „überwiegend" sollte daher in § 1 Abs 2 Satz 1 gestrichen werden.**

Auch sieht § 1 Abs 2 des Entwurfs weiters vor, dass die Beschränkungen des Grundrechts auf Datenschutz – insbesondere im Hinblick auf den Zweck, die verarbeiteten Daten und die Art der Verarbeitung – für die betroffene Person „vorhersehbar" sein müssen. Eine solche Vorgabe existiert im jetzigen § 1 DSG nicht und würde auch der DSGVO widersprechen. Besonders im Bereich der Forschung würde dies große Probleme bereiten bzw. äußerst wichtige Flexibilität nehmen, da hier zum Zeitpunkt der Erhebung der Daten der Zweck nicht immer schon gänzlich eingegrenzt werden kann. Dass dies die DSGVO berücksichtigen will, zeigt va EG 33 sehr deutlich:

> *„Oftmals kann der Zweck der Verarbeitung personenbezogener Daten für Zwecke der wissenschaftlichen Forschung zum Zeitpunkt der Erhebung der personenbezogenen Daten nicht vollständig angegeben werden. Daher sollte es betroffenen Personen erlaubt sein, ihre Einwilligung für bestimmte Bereiche wissenschaftlicher Forschung zu geben, wenn dies unter Einhaltung der anerkannten ethischen Standards der wissenschaftlichen Forschung geschieht. Die betroffenen Personen sollten Gelegenheit erhalten, ihre Einwilligung nur für bestimme Forschungsbereiche oder Teile von Forschungsprojekten in dem vom verfolgten Zweck zugelassenen Maße zu erteilen."*

Die „Vorhersehbarkeit" sollte daher aus Abs 2 gestrichen werden.

iv

B. Zu § 3 (Berichtigungs- und Löschungspflichten)

Hinsichtlich der Berichtigungs- und Löschungspflichten sollte in § 3, angelehnt an § 35 Abs 1 des deutschen Datenschutz-Anpassungs-und Umsetzungsgesetzes, **folgende "Angemessenheitsregelung" ergänzt werden:**

> *"Ist eine Löschung im Falle nicht automatisierter Datenverarbeitung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich und ist das Interesse der betroffenen Person an der Löschung als gering anzusehen, besteht das Recht der betroffenen Person auf und die Pflicht des Verantwortlichen zur Löschung personenbezogener Daten gemäß Artikel 17 Absatz 1 der Verordnung (EU) 2016/679 ergänzend zu den in Artikel 17 Absatz 3 der Verordnung (EU) 2016/679 genannten Ausnahmen nicht. In diesem Fall tritt an die Stelle einer Löschung die Einschränkung der Verarbeitung gemäß Artikel 18 der Verordnung (EU) 2016/679. Die Sätze 1 und 2 finden keine Anwendung, wenn die personenbezogenen Daten unrechtmäßig verarbeitet wurden."*

C. Zu § 4 (Verschwiegenheitspflicht des Datenschutzbeauftragten)

Nach den Erläuterungen zu § 4 soll die Verschwiegenheitspflicht des Datenschutzbeauftragten nicht gegenüber der Datenschutzbehörde gelten. Dessen ungeachtet gilt trotz allem das Bankgeheimnis, das nicht durch einen Satz in den Erläuterungen aufgehoben werden kann. **Die Geltung des Bankgeheimnisses gegenüber der Datenschutzbehörde sollte daher in den Erläuterungen zu § 4 klargestellt werden.**

D. Zu § 7 (Datenschutzbehörde)

Aufgrund der hohen Strafdrohung der DSGVO erscheint die **Vereinigung von Ankläger und Richter in einer Behörde als (verfassungsrechtlich) höchst problematisch**.

Dieses Problem hat sich auch im Kartell- und Wettbewerbsrecht gestellt, welches durch eine Trennung – BWB als Ermittler und Ankläger und das Kartellgericht als Richter – gelöst wurde. Diese Möglichkeit lässt auch die DSGVO offen – die Datenschutzbehörde könnte aufgrund ihrer Sachkompetenz die Rolle der Anklägerin einnehmen und die Verhängung von Geldbußen beim Bundesverwaltungsgericht beantragen, welches dann die Geldbuße zu verhängen hätte.

E. Zu § 10 (Listen bzgl Datenschutz-Folgenabschätzung)

Die IV begrüßt, dass die Datenschutzbehörde nach § 10 auch eine Liste jener Arten von Verarbeitungsvorgängen zu erstellen hat, für die keine Datenschutz-Folgeabschätzung erforderlich ist (Art 35 Abs 5 DSGVO), da dies einen wesentlichen Beitrag zu mehr Rechtssicherheit leistet.

Vor dem Hintergrund des mit einer Datenschutz-Folgeabschätzung verbundenen Aufwandes regt die IV an, die Liste jedenfalls zeitgerecht vor bzw. zum Inkrafttreten der DSGVO kundzumachen. Sie sollte zumindest die Verarbeitungsvorgänge der bisherigen Standard- bzw. Musterverordnung widerspiegeln.

F. Zu § 12 Abs 2 (Veröffentlichung von Entscheidungen)

Nach § 12 Abs 2 sind lediglich *„Entscheidungen der Datenschutzbehörde von grundsätzlicher Bedeutung für die Allgemeinheit"* in geeigneter Weise zu veröffentlichen. Aufgrund der Wichtigkeit des Themas und zur Hilfe der Orientierung in all den sich aus der DSGVO ergebenden Verpflichtungen und Rechten, wäre eine **Veröffentlichung (zumindest der Kurzsprüche) aller Entscheidungen der Datenschutzbehörde unter Gewährleistung entsprechender Anonymisierungen hilfreich.**

G. Zu § 14 (Bestreitungsvermerk)

Ob ein nach § 14 Abs 2 zu setzender „Bestreitungsvermerk" in allen IT-Anwendungen der betroffenen Unternehmen möglich ist, erscheint fraglich. Daher sollte § 14 Abs 2 erster Satz wie folgt ergänzt werden:

*„Ist in einem Verfahren die Richtigkeit von personenbezogenen Daten strittig, so ist vom Beschwerdegegner **im Rahmen seiner technischen Möglichkeiten** bis zum Abschluss des Verfahrens ein Bestreitungsvermerk anzubringen."*

H. Zu § 17 (Vertretung von betroffenen Personen)

Es wird ausdrücklich begrüßt, dass der österreichische Gesetzgeber in dem vorliegenden Entwurf keinen Gebrauch der Öffnungsklausel des Art 80 Abs 2 DSGVO macht und eine Vertretung nur im Auftrag der betroffenen Person vorsieht.

Der Entwurf enthält jedoch keine Regelung darüber, **welche (Qualitäts-)Kriterien derartige Organisationen erfüllen müssen – z.B. Durchlauf einer speziellen Akkreditierung. Der Entwurf sollte daher in diesem Punkt (allenfalls in den Erläuterungen) ergänzt werden.**

I. Zu § 19 (Verhängung von Geldbußen)

Sehr begrüßt wird aus Sicht der IV der – für das österreichische Verwaltungsstrafverfahren – neue Zugang der DSGVO, die juristische Person statt der natürlichen zu bestrafen. Dies erscheint aufgrund des enormen Strafrahmens auch geboten und geht auch auf eine immer größer werdende Herausforderung der Wirtschaft ein: Mitarbeiter bzw. Bewerber sind zunehmend nicht mehr bereit das Damoklesschwert der in Österreich mittlerweile – nicht nur im Datenschutzbereich – enormen Verwaltungsstrafen zu übernehmen.

Um die Verantwortlichkeit der juristischen Personen klar zu verankern, sollte daher in Abs 1 und 2 das „kann" durch ein „hat" ersetzt werden.

Um in weiterer Folge eine Doppelbestrafung von juristischer und natürlicher Person zu vermeiden, erscheint es geboten, den Abs 3 wie folgt abzuändern:

„(3) Die Datenschutzbehörde hat von der Bestrafung eines Verantwortlichen gemäß § 9 des Verwaltungsstrafgesetzes 1991 – VStG, BGBl. Nr. 52/1991, abzusehen, wenn für denselben Verstoß bereits eine Verwaltungsstrafe gegen die juristische Person verhängt wird ~~***und keine besonderen Umstände vorliegen, die einem Absehen von der Bestrafung entgegenstehen.***~~*"*

Da jedoch auch das existenzbedrohende Ausmaß der Geldbußen für natürliche Personen nicht außer Acht gelassen werden sollte, erscheint es im Sinne der Wahrung des richtigen Augenmaßes hilfreich, folgenden Teil des Erwägungsgrundes 150 der DSGVO in die Erläuterungen zu § 19 aufzunehmen:

„Werden Geldbußen Personen auferlegt, bei denen es sich nicht um Unternehmen handelt, so sollte die Aufsichtsbehörde bei der Erwägung des angemessenen Betrags für die Geldbuße dem allgemeinen Einkommensniveau in dem betreffenden Mitgliedstaat und der wirtschaftlichen Lage der Personen Rechnung tragen."

Nach § 19 Abs 5 können gegen Behörden und öffentliche Stellen keine Geldbußen verhängt werden. **Eine Definition des Begriffs „öffentliche Stellen" wäre zur Klarstellung wünschenswert.**

Im Zusammenhang mit der Verhängung von Geldbußen wird die Thematik des Regresses im vorliegenden Entwurf nicht berücksichtigt. Solche Regelungen zu einem möglichen Regress bzw. Schranken desselben wären wünschenswert.

J. Zu §§ 25 ff (Datenverarbeitung zu spezifischen Zwecken)

Um den ohnedies schon enormen bürokratischen Aufwand für Unternehmen nicht unnötig zu erhöhen, **sollte von der Öffnungsklausel des Art 23 DSGVO Gebrauch gemacht werden. Als Vorbild einer sinnvollen und angemessenen Einschränkung kann hier der Entwurf des deutsches Datenschutz-Anpassungs-und Umsetzungsgesetzes herangezogen werden**, welches in § 26 explizit regelt, in welchen Fällen die Verarbeitung von Mitarbeiterdaten zulässig ist. §§ 30 f enthalten weiters Regelungen zu Bonitätsbewertung und Scoring.

Ähnliches ist zu den Betroffenenrechten anzumerken, zu denen §§ 32 ff des deutschen Entwurfs beispielsweise folgende Beschränkungen vorsehen, deren Verankerung auch im österreichischen DSG umgesetzt werden sollte:

- Das Informationsrecht ist eingeschränkt, wenn dadurch die Geltendmachung oder Verteidigung von Rechtsansprüchen beeinträchtigt oder die vertrauliche Mitteilung an öffentliche Stellen gefährdet wäre.

- Das Auskunftsrecht ist eingeschränkt, wenn die Datenspeicherung nur zur Erfüllung von Aufbewahrungsvorschriften oder zur Datensicherung oder Datenschutzkontrolle erfolgt.
- Die Löschungspflicht ist eingeschränkt, wenn die Löschung nur mit unverhältnismäßigem Aufwand möglich wäre und das Interesse des Betroffenen als gering anzusehen ist.

K. Zu § 29 (Verweis auf das ArbVG)

Art 88 Abs 1 DSGVO bietet die Möglichkeit, spezifischere Vorschriften zum Beschäftigtendatenschutz zu treffen – also solche, die der DSGVO bzw. DSG vorgehen, weil sie die dortigen Bestimmungen genauer regeln und somit ersetzen. § 29 des Entwurfs nennt nun als solche Vorschrift iSd Art 88 DSGVO das ganze ArbVG (Arbeitsverfassungsgesetz).

Es wurden schon in der Vergangenheit rege Diskussionen über das Verhältnis zwischen DSG und ArbVG geführt. Auch das ArbVG behandelt zwar Themen mit einer datenschutzrechtlichen Relevanz, allerdings ersetzen die Vorschriften des ArbVG meist nicht die des DSG, sondern es sind beide weiterhin parallel zu prüfen. Unter anderem wurde die Meinung vertreten, dass nach der sog. „Trennungsthese" die datenschutzrechtliche Zulässigkeit unabhängig von der betriebsverfassungsrechtlichen Komponente zu beurteilen ist. Die Zulässigkeit einer Maßnahme nach Datenschutzrecht sagt daher nichts über die Zulässigkeit einer Maßnahme nach Arbeitsverfassungsrecht aus und umgekehrt.

Da die Bestimmungen des ArbVG also (meist) nicht die der DSGVO bzw. DSG ersetzen können und daher weiterhin beide Gesetze parallel zu prüfen sind, erfüllt es den durch Art 88 DSGVO intendierten Zweck der „spezifischeren Vorschriften" nicht. **Aus Sicht der IV ist der Verweis auf das ArbVG daher nicht haltbar, weswegen § 29 zu streichen ist.**

L. Zu § 50 (Protokollierung)

Die Regelungen zur Protokollierung von Verarbeitungsvorgängen nach § 50 des vorliegenden Entwurfs würden zu erheblichen Praxisproblemen führen. Gemäß Abs 1 ist jeder Verarbeitungsvorgang in geeigneter Weise so zu protokollieren, dass die Zulässigkeit der Verarbeitung nachvollzogen und überprüft werden kann. Gemäß Abs 2 sind in automatisierten Verarbeitungssystemen alle Verarbeitungsvorgänge in automatisierter Form zu protokollieren. Die Erläuterungen zu § 50 verweisen auf den folgenden Wortlaut des Art 25 DSGVO:

> *„Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und*

organisatorische Maßnahmen — wie z. B. Pseudonymisierung — trifft, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen."

Aus dieser Bestimmung geht klar ein risikobasierter Ansatz hervor, der sich allerding nicht in den pauschalen Verpflichtungen des Abs 1 und Abs 2 widerspiegelt.

In dieser Schärfe ist diese Regelung des § 50 nicht administrierbar, werden doch die Mitarbeiter eines Verantwortlichen zu erheblichem Dokumentationsaufwand verpflichtet. Die Regelung des Abs 5, wonach der Verantwortliche und der Auftragsverarbeiter der Datenschutzbehörde auf Verlangen die Protokolle zur Verfügung zu stellen hat, findet zudem in der DSGVO keine Entsprechung. **Die gesamte Bestimmung ist aus Sicht der IV daher zu streichen, zumindest aber auf die Verarbeitung sensibler Daten einzuschränken.**

M. Zu § 69 (Verwaltungsstrafbestimmung)

Nach § 69 Abs 2 ist bereits die versuchte Verwirklichung der in § 69 Abs 1 Z 1 – 5 genannten Delikte strafbar. Bei der Einschauverweigerung gegenüber der Datenschutzbehörde ist jedoch völlig unklar, worin der Versuch bestehen soll. **Es bedarf der Klarstellung in den Erläuterungen, dass dieser Tatbestand nicht auch schon bei der Äußerung von bloßen Bedenken verwirklicht sein soll.**

In Anlehnung an das zu § 19 Gesagte, sollte § 69 Abs 3 folgendermaßen abgeändert werden:

*„(3) Gegen juristische Personen **sind ~~können~~** bei Verwaltungsübertretung nach Abs. 1 und 2 Geldbußen nach Maßgabe des § 19 **zu verhängen ~~t werden~~**."*

N. Zu § 76 (Übergangs- und Schlussbestimmungen)

Die DSGVO findet nach ihren Bestimmungen keine rückwirkende Anwendung. Die Regelung des § 76 Abs 5 sieht demgegenüber vor, dass Verletzungen des DSG 2000, die zum Zeitpunkt des Inkrafttretens des Datenschutzanpassungsgesetzes 2018 noch nicht anhängig gemacht wurden, nach der Rechtslage nach Inkrafttreten des Datenschutzanpassungsgesetzes 2018 zu beurteilen sind. Dies steht in einem Spannungsverhältnis zu Artikel 7 der Europäischen Menschenrechtskonvention. **§ 76 Abs 5 sollte daher gestrichen werden.**

O. Bestehende Einwilligungen

Eine **Klarstellung im Sinne des Beschlusses des Düsseldorfer Kreises** (= Konferenz der deutschen unabhängigen Datenschutzbehörden des Bundes und der Länder) vom 13./14. September 2016 zur Fortgeltung bisher erteilter Einwilligungen wäre wünschenswert. Er

besagt: *„bisher erteilte Einwilligungen gelten fort, sofern sie der Art nach den Bedingungen der Datenschutz-Grundverordnung entsprechen (EG 171, Satz 3 DSGVO).* ***Bisher rechtswirksame Einwilligungen erfüllen grundsätzlich diese Bedingungen.****"*.

Jedenfalls aber sinnvoll, wäre eine Klarstellung (so wie ebenfalls Düsseldorfer Kreis), dass die **Informationspflichten nach Artikel 13 DSGVO dafür nicht erfüllt sein müssen**, da sie keine Bedingungen im Sinne des EG 171 sind.

Weiters wäre eine Klarstellung in den Erläuterungen anzuregen, ob und wenn ja unter welchen Bedingungen eine Einwilligung in AGB (weiterhin) möglich ist.

P. Standardvertragsklauseln

Nach dem Wortlaut des Begutachtungsentwurfs ist nicht ausdrücklich vorgesehen, dass die Datenschutzbehörde auch Standardvertragsklauseln gemäß Art 28 Abs 8 DSGVO festlegen wird. Nach Ansicht der IV würden solche Standardvertragsklauseln jedoch wesentlich zur Rechtssicherheit beitragen. **Es erscheint daher sinnvoll, die Aufgaben der Datenschutzbehörde in § 10 um eine entsprechende Verpflichtung zu ergänzen.**

Q. Bedingungen für die Einwilligung eines Kindes

Art 8 Abs 1 DSGVO sieht für die wirksame Einwilligung von Minderjährigen eine Altersgrenze von 16 Jahren vor, die allerdings auf bis zu 13 Jahren herabgesetzt werden kann. Entsprechend der Systematik der im österreichischen Recht geltenden Altersgrenzen sollte der österreichische Gesetzgeber von dieser **Öffnungsklausel Gebrauch machen und die Altersgrenze für eine wirksame eigenständige Einwilligung mit 14 Jahren festlegen.**

Mit diesem Alter sind Jugendliche in Österreich „mündig minderjährig". Mündige Minderjährige dürfen grundsätzlich über ihr Einkommen aus eigenem Erwerb (z.B. Lehrlingsentschädigung) sowie Sachen, die ihnen zur freien Verfügung überlassen worden sind (z.B. Taschengeld), uneingeschränkt bestimmen und sich verpflichten. Damit müssen sie jedenfalls auch in der Lage sein, eine gültige datenschutzrechtliche Einwilligungserklärung abzugeben.

R. Datenschutz-Folgenabschätzung

Es sollte jedenfalls iSd Art 35 Abs 10 DSGVO geregelt werden, dass in jenen Fällen, in denen Verarbeitungen auf gesetzlichen Vorschriften beruhen, keine Datenschutz-Folgeabschätzung notwendig ist. Der Gesetzgeber sollte eine derartige Abwägung ja bereits vor Erlass der entsprechenden Regelung schon selbst getroffen haben.

Es ist beispielsweise unverständlich, dass die Umsetzung der Verordnung über die Vermarktung und Verwendung von Ausgangsstoffen für Explosivstoffe noch zusätzlich eine Folgenabschätzung erfordern könnte – gerade in diesem Fall hat der EU-Gesetzgeber (und

der österreichische Gesetzgeber in der Ausgangsstoffverordnung) die Erfassung und Verarbeitung von Daten über das Interesse des Datenschutzes gestellt. Hier würde bei Fehlen einer solchen Klarstellung den Unternehmen zusätzlich zum bereits bestehenden administrativen Aufwand der Umsetzung (und Dokumentation) unter Umständen auch noch jene der Folgenabschätzung aufgebürdet werden.

Andererseits sollten klare Hinweise auf Granularität, Umfang sowie Ausgestaltung der Datenschutz-Folgenabschätzung aufgenommen werden. Ferner sollte klargestellt werden, ob das Erfordernis einer Datenschutz-Folgenabschätzung nur für neue Verarbeitungssysteme oder wesentliche Veränderungen an bestehenden gilt.

S. Vorherige Konsultation der Datenschutzbehörde

Bei bestimmten Datenanwendungen (z.B.: sensible Datenverarbeitung, Profiling etc) ist nach Art 36 DSGVO eine Vorabkonsultation der Datenschutzbehörde notwendig. Da die DSGVO ab 25. Mai 2018 anzuwenden ist, müsste mit den Vorabkonsultationen bereits vor In-Kraft-Treten des Datenschutz-Anpassungsgesetz begonnen werden.

Um hier eine klare Trennlinie im Hinblick auf den Umfang der Vorabkonsultationen zu schaffen, **sollte eine Übergangsfrist vorgesehen werden, mit der klargestellt wird, dass die Plicht für Vorabkonsultationen nicht für bereits vor dem 25. Mai 2018 bestehenden Datenanwendungen gilt.**

T. Pharmakovigilanz

In dem für die forschende Pharmaindustrie sehr wichtigen Bereich der Pharmakovigilanz (Analyse und Abwehr von Arzneimittelrisiken), wird angeregt, nach Vorbild des deutschen Entwurfs eine **eigene Bestimmung aufzunehmen** (vgl. § 22 Abs 1 lit c dt.).

Bei einer Datenverarbeitung im Rahmen der Pharmakovigilanz, handelt es sich um eine Verarbeitung im öffentlichen Interesse zur Sicherstellung und Überwachung der Gesundheit. Es sollte auch im österreichischen Datenschutzgesetz bzw. in den entsprechenden Materiengesetzen eine Klarstellung getroffen werden, dass die Verarbeitung personenbezogener Daten als Eingriff im öffentlichen Interesse gerechtfertigt ist.

U. Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten

Art 10 DSGVO sieht vor:

> *„Die Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln aufgrund von Artikel 6 Absatz 1 darf nur unter behördlicher Aufsicht vorgenommen werden oder*

wenn dies nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, das geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen vorsieht, zulässig ist. Ein umfassendes Register der strafrechtlichen Verurteilungen darf nur unter behördlicher Aufsicht geführt werden."

Banken sind etwa auf Basis des § 16 Finanzmarkt-Geldwäschegesetz (FM-GwG) iVm § 41 BWG zur Meldung von strafrechtlich relevanten Sachverhalten an die Geldwäschemeldestelle verpflichtet. Diese Regelungen erlauben die Verarbeitung durch Meldung des Kontoinhabers an die Geldwäschemeldestelle. **Es ist aber unklar, ob entsprechende geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen in ausreichender Form vorgesehen sind** (allenfalls käme § 22 FM-GwG in Betracht). **Eine Klarstellung in den Erläuternden Bemerkungen wäre sinnvoll.**

Wir danken für die Kenntnisnahme der Anliegen der Industrie und ersuchen um deren Berücksichtigung.

Mit freundlichen Grüßen
INDUSTRIELLENVEREINIGUNG

Mag. Christoph Neumayer
Generalsekretär

Mag. Alfred Heiter
Bereichsleitung Finanzpolitik & Recht