An das Bundeskanzleramt
Ballhausplatz 2
1014 Wien

E-Mail: v@bka.gv.at
begutachtungsverfahren@parlament.gv.at

Wien, am 21. Juni 2017

BETREFF: ISPA STELLUNGNAHME ZUM ENTWURF EINES BUNDESGESETZES, MIT DEM DAS BUNDES-VERFASSUNGSGESETZ GEÄNDERT, DAS DATENSCHUTZGESETZ ERLASSEN UND DAS DATENSCHUTZGESETZ 2000 AUFGEHOBEN WIRD (DATENSCHUTZ-ANPASSUNGSGESETZ 2018)

Sehr geehrte Damen und Herren,

die ISPA erlaubt sich, in Zusammenhang mit der öffentlichen Konsultation des Bundeskanzleramts zum Entwurf eines Bundesgesetzes, mit dem das Bundes-Verfassungsgesetz geändert, das Datenschutzgesetz erlassen und das Datenschutzgesetz 2000 aufgehoben wird (Datenschutz-Anpassungsgesetz 2018) wie folgt Stellung zu nehmen:

Zunächst begrüßt die ISPA das Bestreben des Gesetzgebers nach möglichst geringen Abweichungen von den Bestimmungen der DSGVO und einer damit einhergehenden Minimalumsetzung der Öffnungsklauseln. Die ISPA ist jedoch der Ansicht, dass die Ausweitung des sachlichen Anwendungsbereichs gegenüber der DSGVO Rechtsunsicherheit bewirkt und näher präzisiert werden sollte. Ferner fordert die ISPA, dass das Mindestalter für eine gültige Einwilligung in die Datenverarbeitung im Zusammenhang mit Diensten der Informationsgesellschaft sich nach der bisherigen Rechtslage richtet um eine Divergenz vom allgemeinen Zivilrecht zu vermeiden. Hinsichtlich des Grundrechts auf Datenschutz spricht sich die ISPA dagegen aus, das Recht auf Löschung im Verfassungsrang zu verankern und hat zudem Bedenken gegenüber einer Übernahme der Zulässigkeitstatbestände der DSGVO als Eingriffstatbestände. Ferner widerspricht die Verhängung der vorgesehenen Geldbußen nach dem Verwaltungsstrafrecht dem Grundrecht auf den gesetzlichen Richter. Die ISPA fordert zudem eine Präferenz der In-Anspruchnahme juristischer Personen gegenüber der Geschäftsführung. Daneben ist auch das Verhältnis der einzelnen Strafbestimmungen zueinander unklar und widerspricht dem Bestimmtheitsgebot. Hinsichtlich der örtlichen Zuständigkeit besteht nach Ansicht der ISPA eine Rechtslücke, die im Rahmen des österreichischen Begleitgesetzes geschlossen werden soll. Eine Beratungs- bzw. Manduktionspflicht der Datenschutzbehörde ist außerdem zumindest in der Übergangsphase auch gegenüber Unternehmen sowie in Zusammenhang mit der Arbeit von CIRTs bzw. CERTs notwendig. Zudem ist die ISPA der Ansicht, dass die vorgesehene Einschränkung der Zurverfügungstellung und Verarbeitung von Adressen nicht der DSGVO entspricht und fordert, dass das öffentliche Interesse an der Transparenz von Daten in öffentlichen Registern gewahrt wird. Darüber hinaus fordert die ISPA die Verarbeitung personenbezogener Daten zum Zwecke der nationalen Sicherheit, des Nachrichtendienstes und der militärische

ISPA – Internet Service Providers Austria
Währingerstrasse 3/18, 1090 Wien, Austria
+43 1 409 55 76
office@ispa.at
www.ispa.at

UniCredit Bank Austria AG
Konto-Nr.: 00660 491 705, **BLZ:** 12000
BIC: BKAUATWW
IBAN: AT59 1200 0006 6049 1705

UID-Nr.: ATU 54397807
ZVR-Zahl: 551223675

Eigensicherung in die Definition der „zuständigen Behörden“ in § 35 Z 7 aufzunehmen sowie eine einheitliche Definition des Terminus „Verantwortlicher“ auch im 3. Hauptstück zu gewährleisten und die Einschränkung des „soweit möglichen“ in § 37 restriktiv einzusetzen um den Regelungsgehalt der Bestimmung nicht zu unterlaufen. Die ISPA empfiehlt zudem in § 36 Abs. 1 Z 2 sowie § 77 Abs. 2 redaktionelle Anmerkungen vorzunehmen. Abschließend sieht die ISPA die Abkürzung der Begutachtungsfrist als demokratiepolitisch höchst bedenklich an.

1) Die Ausweitung des sachlichen Anwendungsbereichs in § 2 bewirkt Rechtsunsicherheit

Der sachliche Anwendungsbereich soll gemäß § 2 des Entwurfs, auf alle (teil-) automatisierten Datenverarbeitungen[1] ausgeweitet werden. Davon ausgenommen sollen demnach nur jene Datenverarbeitungsprozesse sein, die in den Anwendungsbereich des 3. Hauptstücks, die Datenverarbeitung im Rahmen der Strafverfolgung, fallen (Art 2 Abs. 2 lit. d) DSGVO.

Aus den Erläuterungen hierzu geht hervor, dass der Gesetzgeber damit den Anwendungsbereich auch auf Bereiche außerhalb des Anwendungsbereichs des Unionsrechts ausdehnen will, die grundsätzlich aufgrund des Subsidiaritätsprinzips nach Art 2 Abs. 2 lit. a DSGVO vom Anwendungsbereich der Verordnung ausgenommen wären.

Die aktuelle Formulierung des § 2 DSG muss jedoch so interpretiert werden, dass auch die Ausnahme für private Tätigkeiten in Art 2 Abs. 2 lit. c DSGVO, durch das DSG aufgehoben wäre und sohin auch private (teil-) automatisierte Datenverarbeitungen in den Anwendungsbereich fallen würden.

Den weiteren Ausführungen des Gesetzgebers, insbesondere in den Erläuterungen zu § 30 DSG ist zwar zu entnehmen, dass sehr wohl angedacht ist, diese Ausnahmebestimmung aufrecht zu erhalten, eine entsprechende Klarstellung im Rahmen von § 2 DSG wäre jedoch nach Ansicht der ISPA unbedingt notwendig.

2) Das zulässige Mindestalter soll sich nach der bisherigen Rechtslage richten

Das Recht auf Datenschutz als Ausformung des Rechts auf Privatsphäre stellt ein höchstpersönliches Recht dar. Jede Verfügung über eine solche Rechtsposition stellt ebenfalls die Ausübung eines höchstpersönlichen Rechts dar, die grundsätzlich keinem anderen übertragen werden kann. Für ihre Ausübung ist vielmehr die natürliche Einsichts- und Urteilsfähigkeit erforderlich. Fehlt diese Einsicht, so kann ein höchstpersönliches Recht weder durch gesetzliche Vertreter oder Sachwalter noch durch das Pflegschaftsgericht ersetzt werden.

[1] Sowohl die automatisierte Verarbeitung personenbezogener Daten als auch die manuelle Verarbeitung von personenbezogenen Daten, wenn die Daten in einem Dateisystem gespeichert sind oder gespeichert werden sollen

Gemäß aktueller österreichischer Rechtsprechung[2] gibt es nach österreichischem Recht daher keine klare Altersgrenze für Einwilligungen im Zusammenhang mit höchstpersönlichen Rechten, vielmehr sind diese stets in Abhängigkeit von Alter, Entwicklungsstand und Tragweite der Entscheidung zu beurteilen.

Aus den allgemeinen Erläuterungen geht hervor, dass hinsichtlich der Altersgrenze für die Einwilligung eines Kindes in Bezug auf die Datenverarbeitung im Rahmen von Diensten der Informationsgesellschaft bewusst kein Gebrauch von der Öffnungsklausel in Art 8 Abs.1 DSGVO gemacht wurde, da in den Vorgaben der Verordnung bereits ein allgemeiner Ansatz gesehen wird, der in das nationale Recht übernommen werden soll. Demnach würde in Zukunft das Mindestalter für zulässige Einwilligungen bei 16 Jahren liegen, andernfalls ist die Einwilligung durch den Träger der elterlichen Verantwortung notwendig.

Für das Zustandekommen des Grundgeschäfts gelten hingegen die allgemeinen zivilrechtlichen Regelungen (vgl Art 8 Abs. 3 DSGVO). Demnach kann ein mündiger Minderjähriger[3] kleine Anschaffungen selbstständig tätigen und sich in diesem Rahmen auch verpflichten. Die Betragshöhe hängt dabei von einem möglichen Einkommen des Jugendlichen (bspw. aus einer Lehre, Sommerjob) oder dem Taschengeld oder Geburtstagsgeld ab. Ein Vertrag über einen Dienst der Informationsgesellschaft, beispielsweise der Kauf einer App um einige Euros wäre daher zivilrechtlich jedenfalls zulässig.

Als Folge der vorgesehenen Regelung wäre jedoch eine gleichzeitig abgegeben Einwilligung in die Datenverarbeitung, auch eines bereits ausreichend einsichtsfähigen Minderjährigen, ungültig und eine Verarbeitung personenbezogener Daten dementsprechend nicht zulässig. Dies hätte zur Folge, dass die In-Anspruchnahme von Diensten der Informationsgesellschaft auch im kleinen Rahmen, welche in der heutigen Zeit jedenfalls zu den alltäglichen Geschäften eines unter 16-Jährigen gehören, ohne Zustimmung der Eltern nicht mehr zustande kommen könnte, da der Unternehmer seine vertragliche Verpflichtung aufgrund mangelnder Einwilligung nicht erfüllen könnte.

Wie bereits in ErwGr 38 DSGVO richtigerweise erkannt wird, wäre eine weitere Folge dieser Regelung, dass speziell Seelensorgedienste welche über Online-Plattformen angeboten werden, ihre Dienste nicht mehr effektiv anbieten könnten, wenn Kinder sich aufgrund von Problemen mit ihren Eltern an diese richten wollen, da auch hier, nach der vorgesehenen Rechtslage eine Einwilligung der Eltern erforderlich wäre. Der europäische Gesetzgeber hat sich mit diesem Problem befasst und festgehalten, dass die Einwilligung des Trägers der elterlichen Verantwortung im Zusammenhang mit Präventions- oder Beratungsdiensten, die unmittelbar einem Kind angeboten werden, nicht erforderlich sein soll. Aufgrund der mangelnden Bindungswirkung der Erwägungsgründe und zur rechtlichen Klarstellung wäre die Aufnahme einer entsprechenden Bestimmung in das österreichische Recht notwendig.

[2] Vgl OGH 13.01.2016, 15OS176/15v
[3] Personen zwischen 14 und 18 Jahren

Die ISPA spricht sich darum für eine Beibehaltung der bisherigen, auf den Einzelfall abstellenden Herangehensweise aus. Dies würde auch dem grundsätzlich in der DSGVO enthaltenen risikobasierten Ansatz entsprechen und eine realitätsnahe Regelung darstellen.

Außerdem stellt sich die Frage, nach den erforderlichen Alters-Verifizierungsmechanismen, welche Unternehmen vorsehen müssen. Da Verstöße gegen Art 8 DSGVO mit besonders hohen Strafen geahndet werden, EUR 20 Mio. oder 4 % des weltweiten Umsatzes, ist in diesem sensiblen Bereich für Unternehmen Klarheit über die notwendigen Vorkehrungen unabdingbar. Die ISPA fordert daher bei Beibehaltung dieser Bestimmung die Datenschutzbehörde dazu auf, entsprechende Vorgaben an Unternehmen bereits rechtzeitig vorab zur Verfügung zu stellen, damit diese rechtzeitig technisch implementiert werden können.

3) Die Verankerung des Rechts auf Löschung im Verfassungsrang ist nicht notwendig

Kern des Grundrechts auf Datenschutz ist das Recht auf Geheimhaltung der personenbezogenen Daten soweit hierfür ein schutzwürdiges Interesse besteht. Es handelt sich um eine Ausformung des Rechts auf Privatsphäre[4], welches in Art. 8 der Europäischen Grundrechtecharta (GRC)[5] eigens festgeschrieben ist. Jedem soll demnach das Recht zukommen, frei zu bestimmen, wem wann welche seiner persönlichen Daten zugänglich gemacht werden. Hierzu soll jede Person auch über das Recht verfügen „[…]*Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken*." Keine Erwähnung findet jedoch das Recht auf Löschung unzulässig verarbeiteter Daten.

Im österreichischen Datenschutzrecht waren die Rechte auf Auskunft, Richtigstellung und Löschung bereits bisher in § 1 Abs. 3 DSG 2000 geregelt. Diese wurden jedoch bewusst in einem separaten Absatz gegenüber dem allgemeinen Anspruch auf Geheimhaltung der personenbezogenen Daten (§ 1 Abs.1 DSG 2000) geregelt, mit der Voraussetzung „*nach Maßgabe gesetzlicher Bestimmungen*" vorangestellt.

Daraus folgt, dass ein uneingeschränktes Recht auf Löschung, wie im vorliegenden Entwurf des DSG in § 1 Abs. 1 vorgesehen, bislang weder im österreichischen Datenschutzrecht noch in den internationalen Rechtsgrundlagen vorgesehen war. Das Telos des Grundrechts auf Datenschutz war ursprünglich der sorgsame Umgang mit Daten gewesen, ein absolutes Recht auf Löschung als Begleit- bzw. Durchsetzungsrecht ist davon nicht umfasst.

Zudem ist die Umsetzung des Rechts auf Löschung in der Praxis technisch nicht pauschal realisierbar, insbesondere da nicht klargestellt wird, ab wann ein Datensatz tatsächlich als „gelöscht" gewertet wird. Die vollständige Löschung nur eines einzelnen Datensatzes aus einem Dataset ist kaum zu bewerkstelligen, ohne dabei Gefahr zu laufen auch andere Daten zu schädigen. Dies gilt speziell für ältere Anwendungen bei deren Entwicklung entsprechende technologische Vorkehrungen noch nicht zu berücksichtigt wurden. Zwar ist anzunehmen, dass das Prinzip „Privacy by Design" dazu führen wird, dass in Zukunft vermehrt automatisierte

[4] Vgl. Art 8 Europäische Menschenrechtskonvention
[5] Vgl. Art 8 Europäische Grundrechtecharta

Verfahren zur Löschung von Daten in Anwendungen vorgesehen werden, es ist jedoch nicht zu erwarten, dass bereits ab Mai 2018, alle Datenverarbeitungsprozesse technisch entsprechend ausgeformt sein werden um eine unverzügliche Löschung zu ermöglichen. Speziell kleine und mittelgroße Unternehmen mit verhältnismäßig geringen Kapazitäten, sind nicht in der Lage sämtliche Anwendungen innerhalb der noch ausstehenden Zeit derart umzugestalten und Sicherheit über eine rechtskonforme Ausgestaltung zu erlangen, speziell ohne jegliche Hilfestellung durch die nationalen Aufsichtsbehörden.

Es ist zudem zweifelhaft ob ein solches uneingeschränktes Recht auf Löschung mit der bisherigen Rechtsprechung des Verfassungsgerichtshofs (VfGH) in Einklang stehen würde. In § 28 Abs. 2 DSG 2000 war bis zu dessen Aufhebung durch den VfGH im Jahr 2015[6], ein ebenso pauschales unbedingtes Widerspruchsrecht gegen die Zugänglichmachung von persönlichen Informationen in einer öffentlichen Datenanwendung vorgesehen, unabhängig davon ob es sich dabei um Angaben zum Betroffenen selbst, zu seinen Lebensumständen oder seiner beruflichen Tätigkeit handelt, oder ob es sich etwa um Fakten, um Tatsachenbehauptungen oder um Werturteile über den Betroffenen handelt. Ein solches Widerspruchsrecht ohne jegliche Interessensabwägung zwischen dem Betroffenen einerseits und dem Auftraggeber und der Öffentlichkeit andererseits wurde vom VfGH als verfassungswidrig eingestuft, da es keine Berücksichtigung des Einzelfalls zulasse. Aus diesem Grund wurde § 28 Abs. 2 DSG 2000 auch bereits wenige Jahre nach In-Kraft Treten wieder aufgehoben.

Die ISPA anerkennt zwar das Ansinnen des Gesetzgebers – wie aus den Erläuterungen hervorgeht - das Recht auf Datenschutz verständlicher und kürzer auszuformen. In Anbetracht der fehlenden Grundlage im europäischen Primärrecht einerseits sowie angesichts der jüngsten Rechtsprechung des Verfassungsgerichtshofs welche eine Verfassungswidrigkeit einer solchen Bestimmung nahelegt andererseits, regt die ISPA jedoch an, weiterhin an der bisherigen Formulierung festzuhalten und jedenfalls das Recht auf Löschung nicht uneingeschränkt im Verfassungsrang vorzusehen. Daher spricht die ISPA sich dafür aus, analog zur bisherigen Rechtslage eine Formulierung in § 1 DSG aufzunehmen, welche auf die Ausformung des Rechts in Art 17 DSGVO verweist.. Hierdurch würde es auch zu keiner Schlechterstellung des Betroffenen gegenüber der aktuell vorgesehenen Regelung kommen.

4) Die Eingriffstatbestände in § 1 Abs. 2 entsprechen nicht der DSGVO

In § 1 Abs. 2 werden die Eingriffstatbestände in das Grundrecht auf Datenschutz taxativ aufgezählt. Dabei übernimmt der Gesetzgeber einen Teil der in Art 6 DSGVO vorgesehenen Zulässigkeitstatbestände für eine rechtmäßige Datenverarbeitung und wandelt diese in Eingriffsziele für privatrechtliche Tätigkeiten um. Dies ist nach Ansicht der ISPA kritisch zu werten, da dabei zwei unterschiedliche juristische Konstrukte vermengt bzw. gleichgesetzt werden. Die DSGVO enthält neben den Zulässigkeitstatbeständen noch weitere Bestimmungen um die Rechtmäßigkeit der Datenverarbeitung zu beurteilen, insbesondere das System der

[6] VfGH 08.10.2015, G264/2015

Risikofolgeabschätzung. Im vorliegenden Entwurf wird jedoch nur ein Teil davon, die Zulässigkeitstatbestände, übernommen und diese auch nicht vollständig.

Denn § 1 Abs. 2 sieht weder die Verarbeitung in Erfüllung eines Vertrags noch in Erfüllung einer rechtlichen Verpflichtung vor, und sohin gehend lediglich vier der sechs Voraussetzungen der DSGVO. Daraus folgt, dass die Datenverarbeitung in Österreich gegenüber den Vorgaben der DSGVO eingeschränkt werden würde, da etwa eine Verarbeitung von personenbezogenen Daten auf Grundlage eines Vertrags einen unzulässigen Eingriff in ein Grundrecht bedeuten würde.

Darüber hinaus wird als eines der Eingriffsziele das „*überwiegende berechtigte Interesse eines anderen*“ vorgesehen, welches aus § 1 Abs. 2 DSG 2000 übernommen wurde. Diese Formulierung entspricht zwar dem Grunde nach einer der Voraussetzungen zur rechtmäßigen Datenverarbeitung in der DSGVO[7], weist jedoch einen entscheidenden Unterschied auf: Während nach der DSGVO eine Verarbeitung rechtmäßig ist, sofern sie zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten notwendig ist *und nicht die Interessen oder Grundrechte der betroffenen Person überwiegen*, müssen gemäß § 1 Abs. 2 DSG die *Interessen des Verantwortlichen überwiegen*.

Gemäß dem österreichischen Begleitgesetz wäre eine Verarbeitung personenbezogener Daten demnach – vorausgesetzt es liegt keines der anderen Eingriffsziele vor – ein unzulässiger Eingriff in das Grundrecht auf Datenschutz, solange nicht ein berechtigtes Interesse eines anderen überwiegt. Dieses hat der Verantwortliche demnach auch zu beweisen.

Die entsprechende Bestimmung in Art 6 Abs. 1 lit. f DSGVO sieht jedoch das umgekehrte System vor. Demnach ist die Verarbeitung im berechtigten Interesse des Verantwortlichen oder eines Dritten zulässig, solange nicht die Interessen oder Grundrechte der betroffenen Person überwiegen.

Die sprachlichen Unterschiede führen somit zu einer Umkehr in der Interessens- bzw. Risikoabwägung die bei Beurteilung der Rechtmäßigkeit der Verarbeitung durchzuführen ist.

Nach Ansicht der ISPA ist es zweifelhaft, ob eine derartige Änderung angesichts der Direktwirkung einer Verordnung und mangels Öffnungsklausel in diesem Fall zulässig ist. Grundsätzlich würde dadurch die Intention der Verordnung, gleiche Voraussetzungen zur rechtmäßigen Datenverarbeitung in den Mitgliedstaaten zu schaffen untergraben werden. Die ISPA fordert daher eine Übernahme der Formulierung entsprechend jener aus der DSGVO um ein Abweichen von den europarechtlichen Vorgaben zu vermeiden.

Die ISPA ist davon überzeugt, dass die Voraussetzungen für die Verarbeitung personenbezogender Daten abschließend in der DSGVO geregelt sind. Eine darüber hinausgehende Einschränkung wie vom österreichischen Gesetzgeber vorgesehen widerspricht

[7] (Art 6 Abs. 1 lit. f)erlaubt die Verarbeitung personenbezogener Daten „[…] *zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen* […]“.

daher der Verordnung und ist damit nicht Europarechts-konform. Darum fordert die ISPA, von der Aufzählung der Eingriffsziele für privatrechtliche Tätigkeiten in § 1 Abs. 2 gänzlich abzusehen, da die Voraussetzungen in Art 6 DSGVO ohnehin in Österreich direkt anwendbar sind. Sofern der Gesetzgeber jedenfalls an einer Anführung der Eingriffstatbestände festhalten möchte, so sind diese jedenfalls auf alle in Art 6 DSGVO vorgesehenen Voraussetzungen auszuweiten.

5) Die Verhängung der Geldbußen nach dem Verwaltungsstrafrecht verstößt gegen die Grundrechte

Die Datenschutzbehörde (DSB) erhält zum einen gemäß § 11 Abs. 5 iVm 69 DSG weitreichende Strafbefugnisse wobei unter Verweis auf Art 83 DSGVO Strafen von bis zu 20 Mio. Euro oder 4 % des weltweiten Umsatzes verhängt werden können, sowie zum Anderen die Befugnis, Abhilfemaßnahmen nach Art 58 Abs. 2 DSGVO zu verhängen.

Als Verwaltungsbehörde hat die Datenschutzbehörde dabei die Bestimmungen des Allgemeinen Verwaltungsverfahrensgesetzes (AVG) bzw. des Verwaltungsstrafgesetzes (VStG) einzuhalten, sofern nicht besondere Regelungen der DSGVO (etwa zum Kumulationsprinzip, Strafbemessung, Verjährung) diesen vorgehen. Die Verhängung von derart hohen Strafen war dem VStG jedoch bisher fremd. Dieses ist grundsätzlich zur Ahndung von Ordnungswidrigkeiten bestimmt, wobei zweifelhaft ist, ob bei einem Strafausmaß von bis zu EUR 20 Mio. noch von einer solchen gesprochen werden könne.

Nach bisheriger Rechtsprechung des Verfassungsgerichtshofs[8] würden Strafdrohungen iHv bis zu EUR 20 Mio. jedenfalls zum Kernbereich der Strafgerichtsbarkeit zählen. Die Rechtsprechung erfolgte zwar noch vor der Verwaltungsgerichtsbarkeits-Novelle 2012 und damit vor Einführung der Bundesverwaltungsgerichte weswegen die derzeitige Rechtslage hierzu nicht eindeutig ist. Auch zuletzt ging der VfGH jedoch – zwar ohne Verweis auf eine bestimmte Strafandrohung – weiter von einem Kernbereich der Strafgerichtsbarkeit aus, sofern „der Gesetzgeber ein Verhalten als hoch sozialschädlich wertet“[9].

Aufgrund der Höhe der Strafen sowie ihrem Präventions- und Repressivzweck sind die vorgesehenen Geldbußen als Strafen im Sinne des Art 6 EMRK zu werten, dies folgt aus der Rechtsprechung sowohl des EuGH als auch des EGMR[10], weswegen die entsprechenden Verfahrensgrundsätze gewährleistet werden müssen, sowohl hinsichtlich der Verfahrensrechte, als auch des Instanzenzugs. Im Vergleich mit der Strafprozessordnung (StPO) mangelt es dem Verwaltungsstrafrecht jedoch an vielen Verfahrensrechten. Insbesondere ist kritisch zu werten, dass die Datenschutzbehörde als Verwaltungsstrafbehörde im Verfahren sowohl als Ankläger als auch als Richter auftritt (Inquistitionsprinzip), dies widerspricht dem Anklageprinzip im Strafverfahren. Zudem muss sich der Beschuldigte de facto frei beweisen (Beweislastumkehr in § 5 Abs.1 VStG), entgegen der grundsätzlichen Unschuldsvermutung im Strafverfahren. Daneben gelten auch nicht die Grundsätze der Öffentlichkeit, Unmittelbarkeit und Mündlichkeit.

[8] VfGH 29.11.1995, G115/93
[9] VfGH 10.03.2015, G203/2014
[10] Vgl. EGMR 8.6.1976, *Engel and others v. the Netherlands, Rz 87 ff* bzw. Council of Europe (2014): *Guide on Article 6 of the European Convention on Human Rights* S. 7 ff sowie EuGH Rs C-617/10 (Åkerberg Fransson)

Die ISPA regt daher ein Verfahren entsprechend jenem im Kartellrecht an, insbesondere da dieser Rechtsbereich ähnlich hohe Strafen kennt und auf europäischer Ebene gewissermaßen als Vorbild für die Strafhöhe genommen wurde. Im Kartellrecht übernimmt die Bundeswettbewerbsbehörde zwar das Ermittlungsverfahren, Entscheidungen ergehen jedoch vor dem Kartellgericht. Es handelt sich dabei zwar auch nicht um ein Verfahren vor dem Strafgericht, vielmehr entscheidet das Kartellgericht im Verfahren außer Streit. Dies ist jedoch auch nicht zwingend notwendig, da nicht ein tatsächliches Verfahren vor dem Strafgericht notwendig ist, sondern vielmehr die Einhaltung der Verfahrensgrundsätze eines Strafverfahrens an sich. Eine ähnliche Konstruktion in der die Datenschutzbehörde grundsätzlich die Ermittlungsbefugnis samt Verhängung temporärer Abhilfemaßnahmen zukommt, einem Gericht jedoch die Verhängung von Strafen, zumindest ab einer bestimmten Höhe obliegt wäre nach Ansicht der ISPA zu präferieren.

Dies wäre auch im Sinne der DSGVO umsetzbar. Zwar geht die DSGVO grundsätzlich davon aus, dass Geldbußen von Verwaltungsbehörden zu verhängen sind, jedoch ist in Art 83 Abs. 9 DSGVO eine Öffnungsklausel vorgesehen, die es Mitgliedstaaten, deren Rechtsordnung keine Geldbußen vorsehen, ermöglicht, dass die Geldbuße von der zuständigen Aufsichtsbehörde in die Wege geleitet und von den zuständigen nationalen Gerichten verhängt wird. Zwar wurde diese Bestimmung, gemäß ErwGr 151 grundsätzlich in Anbetracht der Rechtsordnungen von Estland und Dänemark vorgesehen, dies bedeutet jedoch nicht, dass nicht auch andere Mitgliedstaaten von dieser Öffnungsklausel Gebrauch machen können, weswegen der Text in Art 83 Abs. 9 DSGVO auch entsprechend allgemein gehalten ist. Wie bereits einleitend ausgeführt, kenn die österreichische Rechtsordnung zwar die Verhängung von Geldbußen, jedoch nur aufgrund von Ordnungswidrigkeiten und nicht wegen schweren Verstößen mit entsprechend hohen Strafdrohungen. Solche Strafdrohungen gehören grundsätzlich zum Kernbereich der Strafgerichtsbarkeit, woraus wiederum folgt, dass das österreichische Recht die Verhängung von Geldbußen wie in Art 83 DSGVO vorgesehen gerade nicht kennt.

Darum müsste nach Ansicht der ISPA auch der österreichische Gesetzgeber, mangels einer Alternative, von der Möglichkeit eines solchen „Splitting“ – Ansatzes Gebrauch machen, um auf diese Weise den Besonderheiten des nationalen Rechts sowie Art 6 EMRK Rechnung zu tragen.

Alternativ, schlägt die ISPA eine Anlehnung an das Finanzstrafverfahren vor. Dort wird in § 53 FinStrG deutlich die Abgrenzung zwischen der gerichtlichen und der finanzstrafbehördlichen Zuständigkeit festgelegt, wobei grundsätzlich für geringe Vergehen die Behörde, darüber hinaus das Gericht zuständig ist. Umgelegt auf das DSG würde dies bedeuten, die DSB wäre Strafbehörde bei Verstößen gegen die taxativ aufgezählten Tatbestände in § 69 DSG, sowie bei geringfügigen Verstößen gegen die Tatbestände nach Art 83 DSGVO. Kommt die Behörde zu dem Ergebnis, es wäre eine Strafe von über EUR 150.000 zu verhängen, müsste sie das Verfahren an das zuständige Gericht verweisen.

6) Die Geldbußen sollen primär gegenüber juristischen Personen verhängt werden

In § 69 Abs. 3 iVm 19 DSG wird, angelehnt an § 99d BWG die Möglichkeit vorgesehen, zukünftig Geldbußen gegenüber juristischen Personen zu verhängen, sofern entweder, ein leitendes Organ den Verstoß begangen hat oder dieser Verstoß aufgrund mangelnder Kontrolle oder Überwachung der Mitarbeiter erfolgt ist.

Gemäß der Formulierung in § 19 Abs. 1 DSG handelt es sich hierbei jedoch um eine „kann" Bestimmung, dies würde die Interpretation nahe legen, dass es der DSB überlassen bleibt die Geldbußen entweder gegenüber der juristischen Person zu verhängen oder sich direkt, in Anwendung von § 69 DSG an die Geschäftsführung zu wenden.

Zwar wird in der DSGVO keine Aussage hinsichtlich einer Präferenz der Bestrafung des Unternehmens oder einer entscheidungsbefugten Person getroffen. Bereits aus den Zielen der Verordnung muss jedoch eine grundsätzliche Präferenz von Geldbußen gegenüber Unternehmen abgeleitet werden. Speziell im Fall von mittelgroßen bis großen Unternehmen, welche zahlreiche unterschiedliche Datenanwendungen betreiben, können gemäß den Bemessungskriterien in Art. 83 Abs. 2 hohe Geldbußen verhängt werden. Es kann jedoch nicht im Sinne des Datenschutzes sein, die Verantwortung dabei an einer einzelnen Person festzumachen und diese in den Privatkonkurs zu treiben. Vielmehr ist es das Ziel der DSGVO, Unternehmen durch entsprechend hohe Strafen aus wirtschaftlichen Erwägungen zur Einhaltung der Bestimmungen zu anzuhalten. Hierfür spricht auch, dass sich Unternehmen im Innenverhältnis wiederum an dem Verantwortlichen regressieren könnten.

Die ISPA spricht sich daher dafür aus, eine Bestimmung in das Gesetz aufzunehmen, welche den Ermessungsspielraum der Behörde hinsichtlich einer In-Anspruchnahme eines Unternehmens oder dessen Geschäftsführung klar regelt und eine Präferenz der In-Anspruchnahme der juristischen Person vorsieht. Dabei handelt es sich auch um keine Einschränkung gegenüber den Vorgaben der DSGVO da diese nur die In-Anspruchnahme eines Verantwortlichen voraussetzt.

7) Das Verhältnis zwischen den einzelnen Straftatbeständen ist unklar

Das DSG sieht in § 69 einen Verwaltungsstrafbestimmung und in § 70 eine Justizstrafbestimmung, vor die im Wesentlichen eine Übernahme der bisherigen Strafbestimmungen in § 50, 51 DSG 2000 darstellen. Da eine Tathandlung unter beide Bestimmungen subsumiert werden kann, wurde das Verhältnis bisher derart geregelt, dass die Verwaltungsstrafe nur anzuwenden ist, sofern der gerichtlich strafbare Tatbestand nicht erfüllt ist. Nunmehr wurde dieses Verhältnis augenscheinlich umgekehrt, indem § 70 DSG darauf verweist, die Bestimmung wäre nur anwendbar „*wenn die Tat nicht mit einer höheren Strafe*" bedacht ist. Grund hierfür sind die in der DSGVO neu eingeführten, hohen Strafbestimmungen iHv bis zu EUR 20 Mio., die direkt anzuwenden sind und durch nationales Recht nicht eingeschränkt werden dürfen. Die Verwaltungsstraftatbestände in § 69 DSG gelten darum auch nur subsidiär gegenüber den Tatbeständen in der DSGVO.

Hinsichtlich einer möglichen Konkurrenz der Tatbestände ist folgendes zu sagen: Eine Tathandlung in der sich jemand widerrechtlich Zugang zu personenbezogenen Daten verschafft hat, diese selbst benützt oder einem anderen zugänglich macht oder veröffentlicht, kann sowohl unter § 70 als auch Art 83 DSGVO subsumiert werden, sofern gleichzeitig Schädigungs- oder Bereicherungsvorsatz gegeben ist, in der Regel wird zumindest Eventualvorsatz gegeben sein. Aufgrund des Doppelbestrafungsverbots würde jedoch eine Geldbuße nach Art 83 DSGVO nicht mehr verhängt werden dürfen, sofern bereits ein rechtskräftiges Urteil aufgrund von § 70 DSG ausgesprochen wurde (Grundsatz des *ne bis in idem*[11]). Dies hätte zur Folge, dass sich der Verantwortliche aufgrund eines Strafverfahrens vor Gericht einer hohen Verwaltungsstrafe entziehen könnte. Dies kann jedoch nicht im Sinne der Förderung des Datenschutzes sein. Aus diesem Grund ist auf das Verhältnis der beiden Straftatbestände zu einander besonderes Augenmerk zu legen.

Da es sich bei den beiden Tatbeständen einerseits um eine Justizstrafe und andererseits um eine Verwaltungsstrafe handelt, ist ein Vergleich des Strafausmaßes, um die Subsidiarität beurteilen zu können, jedoch kritisch zu sehen. Nimmt man das Höchstmaß einer Geldstrafe nach § 70, nämlich 720 Tagessätze á 5000 EUR[12] als Richtwert, so ist entspricht dies einer maximal möglichen Gesamtstrafe iHv EUR 3,6 Mio. Der Betrag ist somit jedenfalls geringer als die Höchststrafe nach Art 83 DSGVO. Demnach würde § 70 DSG jedenfalls immer subsidiär gegenüber einer Geldbuße nach der DSGVO sein.

Einen solchen Vergleich kennt die österreichische Rechtsordnung jedoch bislang nicht und kann dieser nicht ohne weiteres vorausgesetzt werden. Eine Formulierung, die lediglich auf einen Vergleich der Strafausmaße abstellt widerspricht vielmehr aufgrund der unterschiedlichen Art der Strafandrohungen im Verwaltungs- und Justizstrafrecht dem Bestimmtheitsgebot der Art. 18 B-VG. Eine Konsumption einer Justizstrafe kennt die österreichische Rechtsordnung etwa bereits beim Verhältnis von § 52 Glückspielgesetz (GSpG) und § 168 StGB (Verbotenes Glückspiel) wobei hier jedoch § 52 Abs. 3 GSpG klar regelt, dass sofern eine Tat sowohl den Tatbestand der Verwaltungsübertretung nach § 52 als auch den Tatbestand des § 168 StGB verwirklicht nur die Verwaltungsstrafbestimmungen des § 52 zur Anwendung kommen. Eine solche Formulierung ist nach Ansicht der ISPA überzeugender und sollte auch in § 69 DSG aufgenommen werden, sofern von einer Beibehaltung des § 70 DSG ausgegangen wird.

Bei dem gerichtlich strafbaren Tatbestand nach § 51 DSG 2000, der nun in § 70 übernommen werden soll, handelte es sich jedoch schon bisher im Wesentlichen um totes Recht. Insbesondere aufgrund der nun drohenden, hohen Verwaltungsstrafen sieht die ISPA keinen Grund mehr für die Aufnahme eines solchen Straftatbestandes in das DSG. Darum fordert die ISPA den Gesetzgeber dazu auf, von einer Übernahme der Bestimmung in das DSG abzusehen um so mehr Rechtssicherheit zu schaffen sowie andernfalls, jedenfalls eine Klarstellung der Beziehung der beiden Tatbestände zueinander aufzunehmen.

[11] Art 4 Abs. 1 7. ZPEMRK
[12] Das österreichische Strafrecht geht gemäß § 19 Abs.2 StGB von einem maximalen Tagessatz iHv EUR 5000 aus

8) Hinsichtlich der örtlichen Zuständigkeit besteht eine Rechtslücke die im Rahmen des DSG geschlossen werden soll

Art 79 DSGVO sieht für Betroffene die Möglichkeit vor, unmittelbar gegen den Verantwortlichen oder der Auftragsverarbeiter gerichtlich vorgehen zu können, unabhängig eines verfügbaren verwaltungsrechtlichen oder außergerichtlichen Rechtsbehelfs einschließlich des Rechts auf Beschwerde bei einer Aufsichtsbehörde. Hinsichtlich der internationalen Zuständigkeit kann dabei wahlweise auch der Gerichtsstand des Mitgliedstaats gewählt werden, in dem die betroffene Person ihren Aufenthaltsort hat. Der Begriff des „Aufenthaltsorts" existiert bisher aber weder in der österreichischen noch in der europäischen Rechtsordnung, sondern es wurde bislang stets auf den „gewöhnlichen Aufenthaltsort" abgestellt. Aus einem Vergleich mit der englischen Sprachfassung geht hervor (*„habitual residence"*), dass es sich hierbei wohl lediglich um eine unzureichende Übersetzung handelt.

Die DSGVO trifft jedoch lediglich die Aussage über die internationale Zuständigkeit, nicht über die örtliche Zuständigkeit des Gerichts im Mitgliedstaat in der der Betroffene tatsächlich seinen (gewöhnlichen) Aufenthaltsort hat. In dieser Frage besteht eine Gesetzeslücke welche nach Ansicht der ISPA im DSG zu schließen wäre.

9) Eine Beratungs- bzw. Manduktionspflicht wäre auch gegenüber Unternehmen notwendig

Wie in § 10 DSG festgelegt, obliegt der DSB eine der Behördentätigkeit vorgelagerte begleitende Beratungstätigkeit des National- bzw. Bundesrats sowie der Bundes- bzw. Landesregierungen im Rahmen von legislativen und administrativen Maßnahmen. Eine solche Manduktionspflicht gegenüber Unternehmen besteht jedoch nur im Zuge einer verpflichtenden Konsultierung der DSB im Rahmen der Datenschutzfolgeabschätzung.

Wie bereits in einigen der vorangegangenen Punkte angeschnitten, gibt es viele Bereiche in denen Unternehmen Entscheidungen hinsichtlich der technischen Ausformung von Datenverarbeitungsprozessen treffen müssen, ohne jegliche Anhaltspunkte in der Spruchpraxis der Behörde. Insbesondere in der Übergangsphase, in der die Geldbußen bereits in vollem Ausmaß verhängt werden können, sich jedoch noch keine Spruchpraxis der Behörde entwickelt hat, setzen sich die Unternehmen damit einem enormen Risiko aus. Dies könnte zur Folge haben, dass viele österreichische Unternehmen um potentiell existenzbedrohenden Geldbußen zu entgehen, sich äußerst defensiv verhalten werden und im Zweifel von der Fortführung bisheriger oder der Aufnahme neuer innovativer Tätigkeiten absehen werden. Damit würden jedoch der österreichische Wirtschaftsraum sowie speziell das Bestreben Österreichs, die Chancen der Digitalisierung bestmöglich zu nutzen[13] nachhaltig beeinträchtigt werden.

Aus diesem Grund spricht sich die ISPA klar für eine Manduktionspflicht auch gegenüber Unternehmen aus um diese dabei zu unterstützen, ihre wirtschaftliche Tätigkeit unter Einhaltung

[13] Vgl hierzu etwa die Ausführungen in der „Digital Roadmap Austria"

der Datenschutz-Standards weiterhin bestmöglich ausüben zu können. Das potentielle Gegenargument, dass die DSB in einem späteren Verfahren dann an die im Rahmen der Manduktionspflicht getätigten Angaben faktisch gebunden wäre, kann dadurch ausgeräumt werden, dass das Verfahren auf die DSB als ermittelnde Behörde sowie ein Gericht als Entscheidungsinstanz aufgeteilt wird (vgl hierzu bereits die Ausführungen in Punkt 5).

10) Ersuchen um Klarstellung bezüglich der Verwendung von personenbezogenen Daten im Rahmen von Security-Teams und CERTs

Die ISPA ersucht die DSB im Zuge der Umsetzung klarzustellen, inwieweit und unter welchen Umständen Erwägungsgrund 49 der DSGVO folgend die Verwendung von personenbezogenen Daten im Rahmen der Aufgaben von Security-Teams und CERTs zulässig ist, insoweit diese erforderlich ist, um die Sicherheit der Infrastruktur des Betreibers sowie der angeschlossenen Netze und Endgeräte zu gewährleisten und die effektive Reaktion auf Sicherheitsprobleme zu ermöglichen.

11) Die Einschränkung der Zurverfügungstellung und Verarbeitung von Adressen entspricht nicht der DSGVO

§ 26 DSG regelt die Zurverfügungstellung bzw. Verarbeitung von Adressen von Betroffenen zum Zweck ihrer Benachrichtigung oder Befragung. Es handelt sich dabei um die beinahe wortgleiche Übernahme der bisherigen Regelung in § 47 Abs. 4 DSG 2000, wobei jedoch zweifelhaft erscheint, ob diese Bestimmung mit dem Regime der DSGVO konform bzw. überhaupt notwendig ist. Speziell die in Abs. 4 enthaltene Verpflichtung zur Einholung einer Genehmigung bei der DSB entspricht einer Einschränkung gegenüber den allgemeinen Regelungen zur Datenverarbeitung welche keine Grundlage in der DSGVO hat und für die auch sonst keine rechtliche Notwendigkeit besteht.

Der Gesetzgeber gesteht selbst in den Erläuterungen zu § 26 ein, dass spezielle Fragestellungen hinsichtlich der Zurverfügungstellung von Adressen in der Vergangenheit hauptsächlich in Hinblick auf die sogenannte „Geburtstagsgratulation“ aufkamen. Die hierzu notwendige Verarbeitung personenbezogener Daten richtet sich jedoch nach den Vorgaben des Meldegesetzes[14].

Mangels rechtfertigenden Anwendungsbereichs, spricht sich die ISPA daher für eine Streichung von § 26 DSG aus, und fordert im Sinne der Einheitlichkeit, dass die allgemeinen Regelungen der DSGVO hinsichtlich der Datenverarbeitung zur Anwendung kommen.

[14] Meldegesetz 1991, BGBl. Nr. 9/1992

12) Das öffentliche Interesse an der Transparenz von Daten in öffentlichen Registern muss gewahrt werden

In § 27 DSG wird die rechtliche Grundlage für die Verarbeitung von Daten für wissenschaftliche, künstlerische und journalistische Tätigkeiten im Einklang mit dem Recht auf freie Meinungsäußerung geschaffen. Dies entspricht der Verpflichtung zur Umsetzung von Art 85 DSGVO in nationale Rechtsvorschriften. Darüber hinaus bietet die DSGVO jedoch Mitgliedstaaten in Artikel 86 auch die Möglichkeit, den Zugang der Öffentlichkeit zu amtlichen Dokumenten zu regeln. Damit soll ebenso ein Ausgleich zwischen dem Recht auf Informationszugang und dem Recht auf Datenschutz erfolgen und das öffentliche Interesse an der Transparenz amtlicher, öffentlich zugänglicher Dokumente gewahrt sowie die Weiterverwendung von Informationen des öffentlichen Sektors ermöglicht werden.

Erwägungsgrund 154 verweist in Zusammenhang mit der Weiterverwendung der Daten auf die Richtlinie über die Weiterverwendung von Informationen des öffentlichen Sektors (PSI-RL 2003/98/EG), welche in Österreich durch das Informationsweiterverwendungsgesetz (IWG) umgesetzt wurde. Demnach können Daten, die ohne Einschränkung öffentlich zugänglich sind, für kommerzielle und nicht kommerzielle Zwecke weiterverwendet werden. Wie aus den Erwägungsgründen der PSI Richtlinie hervorgeht, soll hierdurch die innovative Nutzung von Daten des öffentlichen Sektors gefördert und an die Anforderungen der Informations- und Wissensgesellschaft angepasst werden. Diese Möglichkeit soll dazu dienen weitere Arbeitsplätze im digitalen Bereich zu schaffen und wird derzeit insbesondere von Startup-Unternehmen wahrgenommen.

Um eine entsprechende Weiterverwendung zu gewährleisten ist es jedoch notwendig, dass Daten in öffentlichen Registern vollständig angezeigt werden. Jeglicher Widerspruch gegen eine Verarbeitung derartiger Daten müsste damit auch mit dem öffentlichen Interesse an möglichst hoher Transparenz von Informationen des öffentlichen Sektors abgewogen werden. Als Beispiele sei hierbei etwa auf die Verwendung von Insolvenzdaten beim Gläubigerschutz oder die Veröffentlichung von Abfalldeponien im Rahmen des Umweltschutzes verwiesen.

Da weder die PSI-RL noch das IWG entsprechende datenschutzrechtliche Bestimmungen enthält, fordert die ISPA daher, dass im Rahmen von § 27 DSG klargestellt wird, dass Betroffene jedenfalls mit der Weiterverwendung ihrer Daten gemäß IWG bzw. PSI-RL zu rechnen haben, wenn sie in öffentlich zugängliche Register eingetragen werden und das öffentliche Interesse im Sinne des Rechts auf Informationszugang bei der möglichen Ausübung eines Widerspruchsrechts gebührend berücksichtigt wird.

13) Die Verarbeitung personenbezogener Daten zum Zwecke der nationalen Sicherheit, des Nachrichtendienstes und der militärische Eigensicherung ist in die Definition der „zuständigen Behörden“ in § 35 Z 7 aufzunehmen.

Beim Anwendungsbereich des 3. Hauptstücks (Verarbeitung personenbezogener Daten für Zwecke der Sicherheitspolizei, des polizeilichen Staatsschutzes, des militärischen Eigenschutzes, der Aufklärung und Verfolgung von Straftaten, der Strafvollstreckung und des Maßnahmen-vollzugs) wird im § 34 auf die Verarbeitung personenbezogener Daten durch zuständige Behörden zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, sowie zum Zweck der nationalen Sicherheit, des Nachrichtendienstes und der militärische Eigensicherung abgestellt.

Im Widerspruch dazu steht der § 35 Z 7 der als 7. „zuständige Behörde“ folgende Definition vornimmt:

> „*a) eine staatliche Stelle, die für die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, zuständig ist, oder*
>
> *b) eine andere Stelle oder Einrichtung, der durch das Recht der Mitgliedstaaten die Ausübung öffentlicher Gewalt und hoheitlicher Befugnisse zur Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder zur Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, übertragen wurde;*“

Somit gäbe es keine „*zuständige Behörde*“ für die Verarbeitung personenbezogener Daten zum Zwecke der nationalen Sicherheit, des Nachrichtendienstes und der militärische Eigensicherung mehr, obwohl dies im § 34 im Anwendungsbereich umfasst ist.

Die ISPA fordert daher, diese in § 35 Z 7 a) aufzunehmen, wodurch diese Bestimmung wie folgend lauten sollte:

> „*a) eine staatliche Stelle, die für die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, sowie zum Zweck der nationalen Sicherheit, des Nachrichtendienstes und der militärische Eigensicherung, zuständig ist, oder*“

14) Es ist eine einheitliche Definition des Terminus „Verantwortlicher“ auch im 3. Hauptstück zu gewährleisten.

Im § 35 Z 8 wird als 8. „Verantwortlicher“ die zuständige Behörde, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet, abschließend definiert, während in der DSGVO sowohl eine Behörde oder Organisation, als auch eine natürliche Person Verantwortlicher sein kann.

Die ISPA spricht sich daher dafür aus, eine einheitliche Definition auch im 3. Hauptstück beizubehalten.

15) Die Einschränkung des „soweit möglichen“ ist restriktiv einzusetzen um den Regelungsgehalt der Bestimmung nicht zu unterlaufen.

Im § 37 Kategorisierung und Datenqualität wird auffallend oft die Formulierung „soweit möglich“ verwendet, die den Bestimmungsgehalt des Gesetzes relativiert. Es ist anzuregen, diese Formulierung ausschließlich dort zu verwenden, wo sie unbedingt notwendig erscheint.

16) In § 36 Abs. 1 Z 2 sowie § 77 Abs. 2 sind redaktionelle Anmerkungen vorzunehmen.

In den Grundsätzen für die Datenverarbeitung § 36 sollte im Abs. 1 Z 2 zwischen den Wörtern „und“ und „nicht“ das Wort „dürfen“ eingefügt werden.

Der Satz sollte dann folgendermaßen lauten:

> *„2. müssen für festgelegte, eindeutige und rechtmäßige Zwecke erhoben und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise verarbeitet werden,“*

Im § 77 (Inkrafttreten) Abs. 2 steht folgende Bestimmung:

> “*(2) (Verfassungsbestimmung) § 1, § 7 Abs. 3 und § 62 Abs. 3 DSG 2000 treten mit 25. Mai 2018 in Kraft. Gleichzeitig treten die §§ 1 bis 3, § 35 Abs. 2, § 60 Abs. 8, § 61 Abs.4 DSG 2000 außer Kraft.*“

Die erste Erwähnung des DSG 2000 scheint ein Tippfehler zu sein. Es sollte daher nach Ansicht der ISPA „Datenschutz-Anpassungsgesetz 2018“ heißen.

17) Die Abkürzung des Begutachtungsverfahrens ist demokratiepolitisch höchst bedenklich

Abschließend möchte die ISPA noch festhalten, dass sie es äußerst bedenklich sieht, dass im Rahmen des Gesetzgebungsprozesses, demokratiepolitische Grundsätze übergangen wurden und der vorliegende Entwurf vor Ende der Begutachtungsfrist am 22.6., bereits im Rahmen der Plenarsitzung am 07.06.2017 als Regierungsvorlage beschlossen wurde. Die Einarbeitung und Berücksichtigung der Stellungnahmen im Rahmen des parlamentarischen Prozesses bietet keinen gleichwertigen Ersatz, da eine Abänderung des Entwurfs in diesem Stadium nur noch erschwert möglich ist.

Speziell da es sich hierbei um ein Rechtgebiet handelt welches im Wesentlichen die Ausübung und den Schutz eines Grundrechts sowie dessen Abwägung mit anderen Rechten behandelt, ist ein transparenter Gesetzgebungsprozess notwendig, an welchem alle beteiligten Stakeholder gebührend berücksichtigt werden können, dies wurde auch von Seiten der Regierung wiederholt betont.

Die ISPA zeigt zwar Verständnis, dass angesichts der anstehenden Neuwahlen im Herbst, das Datenschutz-Anpassungsgesetz 2018 noch zuvor beschlossen werden muss, da andernfalls eine rechtzeitige Umsetzung der Bestimmungen durch die Unternehmen nicht mehr möglich wäre.

Die ISPA ist jedoch davon überzeugt, dass auch unter Zeitdruck, die Einhaltung demokratiepolitischer Grundsätze wie eine transparente Einbeziehung der Stakeholder unumgänglich ist und in diesem Fall auch jedenfalls möglich gewesen wäre. Die ISPA spricht sich klar gegen eine Wiederholung eines solchen Einschnitts in die Beteiligung der Bevölkerung am Gesetzgebungsverfahren in der Zukunft aus.

Für Rückfragen oder weitere Auskünfte stehen wir jederzeit gerne zur Verfügung.

Mit freundlichen Grüßen,

ISPA - Internet Service Providers Austria

Dr. Maximilian Schubert

Generalsekretär

Die ISPA – Internet Service Providers Austria – ist der Dachverband der österreichischen Internet Service-Anbieter und wurde im Jahr 1997 als eingetragener Verein gegründet. Ziel des Verbandes ist die Förderung des Internets in Österreich und die Unterstützung der Anliegen und Interessen von über 200 Mitgliedern gegenüber Regierung, Behörden und anderen Institutionen, Verbänden und Gremien. Die ISPA vertritt Mitglieder aus Bereichen wie Access, Content und Services und fördert die Kommunikation der Marktteilnehmerinnen und Marktteilnehmer untereinander.