Stellungnahme zum Datenschutz-Anpassungsgesetz 2018

Internetoffensive ÖSTERREICH

Bundeskanzleramt-Verfassungsdienst

Ballhausplatz 2

1010 Wien

Per E-Mail v@bka.gv.at.

Präsidium des Nationalrates

begutachtungsverfahren@parlament.gv.at

Wien, am 20.6.2017

BKA-810.026/0019-V/3/2017

Stellungnahme zum

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

Mit der Veröffentlichung dieser Stellungnahme auf der Parlamentshomepage erklären wir uns ausdrücklich einverstanden.

Internetoffensive ÖSTERREICH

Inhalt

Internetoffensive ÖSTERREICH

1. Einleitung

Die Internetoffensive Österreich beehrt sich, ihre Stellungname zum Datenschutz-Anpassungsgesetz 2018 zu übermitteln.

Unsere Stellungnahme zu den Öffnungsklauseln der Datenschutzgrundverordnung wurde bereits im Rahmen des IKT Konvents am 25.1.2017 veröffentlicht. Wir erlauben uns im gegenständlichen Schreiben diese Positionen erneut aufzugreifen, sofern wir nicht bei einzelnen Paragraphen auf diese Anregungen eingehen.

Das Datenschutzrecht hat in Österreich bisher schon ein sehr hohes Schutzniveau für Betroffene geboten. Dennoch wird durch die europäische DSGVO eine wesentliche Verschärfung für alle Unternehmen, die Dienstleistungen in Europa adressieren, angeordnet. Durch zahlreiche Öffnungsklauseln ist es dem österreichischen Gesetzgeber trotz des vorherrschenden Harmonisierungsgedankens möglich, nationale Abweichungen zu regeln. Der Gesetzgeber hat in dem uns vorliegenden Entwurf erfreulicher Weise mit Augenmaß von diesen Gebrauch gemacht.

Dennoch müssen wir feststellen, dass einige Regelungsansätze zu Ungunsten der Österreicher, der österreichischen Wirtschaft und der österreichischen Angestellten und Arbeiter vorgesehen sind. Auf diese Punkte werden wir in der folgenden Stellungnahme detailliert eingehen.

Wir setzen uns gemeinsam für ein möglichst hohes Datenschutzniveau ein, das den Unternehmen jedoch weiterhin ermöglichen muss, die Wirtschaft wachsen zu lassen. Bei der Herausforderung der Implementierung der DSGVO in Österreich sind wir daher auf einen starken Rückhalt aus der Politik angewiesen und dem Verständnis, dass wir alle vor einer großen Herausforderung stehen.

Selbstverständlich stehen wir jederzeit für Rückfragen und weitere Erläuterungen zur Verfügung.

Internetoffensive ÖSTERREICH

Die Stellungnahme wurde im Juni 2017 vom Vorstand der IOÖ angenommen:

gez. Andreas Bierwirth, CEO
T-Mobile Austria GmbH

gez. Michael Butz, Generaldirektor
A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH

gez. Wilhelm Doupnik, CEO
Raiffeisen Informatik GmbH

gez. Nikolaus Futter, Geschäftsführer
Compass-Verlag GmbH

gez. Marcus Frantz, CIO
ÖBB Holding AG

gez. Erwin Greiml, Geschäftsführer
Adesso Austria GmbH

gez. Rainer Kalkbrener, Vorstandsvorsitzender
ACP Holding Österreich GmbH

gez. Harald Leitenmüller, CTO
Microsoft Österreich GmbH

gez. Stefanie Lindsteadt, Univ.- Prof. Dipl.- Inf. Dr.
Technische Universität Graz

gez. Bernhard Nagiller, Geschäftsführer
Internetoffensive Österreich

gez. Michaela Novak-Chaid, Geschäftsführerin
HP Austria GmbH

gez. Marco Porak, Director Financial Services Sector
IBM Österreich

gez. Rudi Richter, COO
SAP Österreich GmbH

gez. Johann M. Schachner, Country Manager Österreich
Atos IT Solutions and Services GmbH

gez. Alexander Schuster, CEO
ZTE Austria GmbH

gez. Norbert Schöfberger, Generaldirektor
Hewlett Packard Enterprise

gez. Gregor Schönstein, Geschäftsführer
Internetoffensive Österreich

gez. Margarete Schramböck, CEO
A1 Telekom Austria AG

gez. Alfred Taudes, Univ.-Prof. Mag. Dr.
Wirtschaftsuniversität Wien

gez. Jan Trionow, CEO
Hutchison Drei Austria GmbH

gez. Hubert Wackerle, Geschäftsführer
IT Services der Sozialversicherungs GmbH

gez. Peter Wukowits, Managing Director
Nokia Austria GmbH

Internetoffensive ÖSTERREICH

2. Management Summary

1. DATENSCHUTZBEHÖRDE und RECHT AUF GESETZLICHEN RICHTER
   § 10 DSG AnpG Beraten statt Strafen – die Datenschutzbehörde sollte in erster Linie beratend tätig werden. Damit einhergehend benötigt die Wirtschaft Rechtssicherheit bei der Verhängung der Strafen. **Wir fordern ein ordentliches Verfahren, bei dem ermittelt wird, die Unternehmen eine Möglichkeit zur Rechtfertigung erhalten und letztendlich ein Gericht über die Strafe entscheidet**!

   Heute sind vergleichsweise geringe Strafen im Verwaltungsrecht vorgesehen, die die jeweiligen Geschäftsführer bzw. Verantwortlichen treffen. Wir begrüßen die Haftung des Unternehmens als juristische Person, halten jedoch angesichts des Strafrahmens von bis zu 4 % des weltweiten Jahresumsatzes ein ordentliches Verfahren für rechtsstaatlich unumgänglich. Dies hätte natürlich den Vorteil, dass die sachkundige Datenschutzbehörde ohne Interessenskonflikt beraten kann. Grundsätzlich sind Unternehmen bestrebt, rechtskonform zu agieren. Manchmal handeln Unternehmen jedoch in „Grauzonen“, bei denen die Bewertung der Behörde nicht antizipiert werden kann, weshalb eine Beratungsfunktion sinnvoll ist. Außerdem muss klargestellt werden, dass gegen eine natürliche Person, gleichgültig ob sie Geschäftsführer, Vorstand oder verantwortlicher Beauftragter iSd VStG ist, keine Strafe verhängt werden darf, wenn für denselben Verstoß eine Verwaltungsstrafe gegen eine juristische Person möglich ist. Damit würde auch sichergestellt werden, dass es in der Regel nicht zu einer Doppelbestrafung von juristischer- und natürlicher Person kommt.

2. **Minderjährige** können in Österreich ab dem Alter von 14 Jahren rechtswirksame Geschäfte tätigen. Das muss ebenfalls für datenschutzrechtliche Einwilligungen gelten! Das Auseinanderklaffen von 14-jährigen, die Apps kaufen dürfen, jedoch für die Einwilligungen in der App ihre Eltern um Erlaubnis bitten müssen, ist nicht durchführbar und schädigt das tägliche Geschäftsleben!
   Wir regen den Gesetzgeber daher dringend an, hier ein einheitliches Alter vorzusehen, ab dem man Kindern zutraut, Geschäfte zu tätigen.

3. **Rechtsgültig erteilte Einwilligungserklärungen müssen weiter gelten**
   Viele Unternehmen - so auch die Telekommunikationsunternehmen - haben in den letzten Jahren von ihren Kunden Einwilligungserklärungen zur Datenverarbeitung eingeholt. Es muss sichergestellt und zumindest in den Erläuternden Bestimmungen geklärt werden, dass diese Einwilligungserklärungen, wenn sie den bisherigen rechtlichen Anforderungen entsprochen haben, auch weiter gelten.

4. **Haftung der Beschäftigten** 50.000 EUR Strafe für Mitarbeiter bei Verletzung von Datengeheimnissen ist erstens viel zu hoch bemessen, da existenzbedrohend, und zweitens führt dies zu einem unangenehmen Arbeitsklima! Mitarbeiter werden minutiös dokumentieren müssen, wann sie welche Anweisung erhalten haben, um sich im Falle des Falles freibeweisen zu können!

Heute drohen Strafen bis zu 10.000 EUR bei vorsätzlichem Verhalten. Fahrlässiges Verhalten der Mitarbeiter wurde durch das Dienstnehmerhaftungsprivileg gedeckt. Die Vorrangigkeit des DN-Haftungsprivilegs muss jedenfalls klargestellt werden.

Des Weiteren muss in § 29 DSG-AnpG die Einschränkung auf datenschutzrechtlich relevante Betriebsvereinbarungen im Sinne von §§ 96 und 96a ArbVG getroffen werden, damit nicht für JEDE nicht abgeschlossene Betriebsvereinbarung plötzlich der hohe Strafrahmen der DSGVO schlagend wird. Hier muss eine Klarstellung im Gesetz getroffen werden, um Betriebe nicht willkürlich in die Pflicht zu nehmen!

Auf den folgenden Seiten gehen wir im Detail auf sämtliche problematische Regelungen ein.

Wir appellieren an einen gemeinsamen Lösungsansatz, bei dem wir zusammen den besten Weg für Österreich, die österreichische Wirtschaft und die österreichischen Arbeiter und Angestellten einschlagen werden.

Beraten statt Strafen – wir möchten nicht die Staatskasse füllen, sondern gemeinsam „best practice“ entwickeln.

Internetoffensive ÖSTERREICH

3. Inhaltliche Bemerkungen[1]

3.1 § 1 Verfassungsbestimmung Grundrecht auf Datenschutz

§ 1 DSGAnpG hebt- wie auch bisher – das Grundrecht auf Datenschutz in den Verfassungsrang, wobei auch das Recht auf Löschung von diesem Grundrecht explizit umfasst sein soll. Im Hinblick auf das in der Europäischen Grundrechtscharta und in der Menschenrechtskonvention verankerte Grundrecht ist die Verfassungsbestimmung bezüglich des Grundrechtes auf Datenschutz selbstredend. Wenn es jedoch um das Recht auf Löschung geht, das gemäß DSGVO eines der – wohl gleichwertig nebeneinander bestehenden – reinen Betroffenenrechte ist, so ist eine Inkludierung in das Grundrecht auf Datenschutz nicht nachvollziehbar und nicht sinnvoll. Vielmehr geht dies über den Anwendungsbereich und die Vorgaben der DSGVO hinaus und widerspricht diesen sogar.

Wir sehen hier also den dringenden Bedarf, die Wortfolge *„…sowie auf Richtigstellung unrichtiger Daten und auf Löschung unzulässiger Weise verarbeiteter Daten“* aus § 1, sowie die entsprechenden Hinweise in den Erläuterungen dazu, ersatzlos zu streichen. Sollte die Bestimmung aus verfassungsrechtlichen Gründen für die Verarbeitung im öffentlichen Kontext erforderlich sein, so schlagen wir als Alternative zu Streichung vor, den gesamten Absatz 1 in das dritte Hauptstück des DSG zu verschieben.

§ 1 Absatz 2 sieht ausdrücklich und taxativ mögliche Eingriffstatbestände in das Grundrecht auf Datenschutz vor. Dies erscheint grundsätzlich gerechtfertigt, zumal es sich um ein relatives und nicht um ein absolutes Grundrecht handelt. Allerdings sehen wir auch hier nicht die Notwendigkeit einer Regelung auf nationaler Ebene, zumal die DSGVO hier direkt ausreichende Regelungen vorsieht. Auch hier wäre eine Streichung geboten bzw. bei Bedarf aus verfassungsrechtlichen Gründen eine Verschiebung in das dritte Hauptstück des DSG tunlich.

Aber auch inhaltlich ist die Regelung des Absatz 2 nicht konform mit der DSGVO: Zunächst ist fraglich, ob man bei den in Absatz 2 genannten Tatbeständen überhaupt von Eingriffstatbeständen sprechen kann. Diese scheinen die in Artikel 6 genannten Rechtfertigungsgründe für eine Datenverarbeitung zu reflektieren, wobei aber im DSG dabei nur 4 von 6 erwähnt werden. Das ist zu hinterfragen. Weiters möchten wir festhalten, dass wir die Bezeichnung „Eingriffstatbestände“ als unangemessen halten, da es hier lediglich um möglich **rechtliche Grundlagen** für die **zulässige** Datenverarbeitungen handelt. Eingriffsrechte ergeben sich aus dem gesamten Kontext der DSGVO, die mit ihrem risikobasierten Ansatz auch keine abschließende Aufzählung von Eingriffstatbeständen zulässt.

In Artikel 6 DSGVO werden neben der Einwilligung der betroffenen Person dessen lebenswichtigen Interessen, das öffentliche Interesse und das Interesse des Verarbeitenden, das nicht von den Interessen der Betroffenen auf Datenschutz überwogen werden darf, die (vorvertragliche) Erfüllung eines Vertrages und die rechtliche Verpflichtung angeführt. Wir sehen hier einen systematischen Bruch in der Einordnung der Tatbestände des Artikels 6 der DSGVO als „*Eingriffstatbestände*“ und empfehlen, diese zu streichen

[1] Sämtliche Verweise auf Paragraphen ohne Angabe der Rechtsvorschrift beziehen sich auf das Datenschutzgesetz-DSG in der Fassung des Entwurfs zum Datenschutz-Anpassungsgesetz 2018.

bzw. der DSGVO entsprechend als **„rechtliche Grundlage“** zu bezeichnen. Alle 6 von der DSGVO aufgezählten Fälle müssen jedenfalls angeführt werden.

Hinweisen möchte wir auch auf den Umstand, dass die Wortfolge „oder im überwiegenden berechtigten Interesse eines anderen zulässig“ in § 1 Abs 2 DSGAnpG nicht der ausdrücklichen und auch intendierten Regelung von Artikel 6 Abs 1 lit f („die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt“) entspricht, in der die Interessensabwägung eben nicht vom berechtigten Interesse des Verarbeitenden abhängt, sondern eben umgekehrt von den Interessen des Betroffenen. Wir sehen hier eine Unvereinbarkeit mit der DSGVO und empfehlen, dies richtig zu stellen.

3.2 Beraten statt Strafen muss auch für die Datenschutzbehörde gelten!

Die Einführung der DSGVO stellt die österreichische Digitalwirtschaft vor enorme Herausforderungen. Es kommen viele neue Pflichten auf Verantwortliche und Auftragsverarbeiter zu, die mit existenzbedrohenden Strafen bedroht werden. Es ist zu erwarten, dass der österreichische Gesetzgeber in so einer Situation die betroffenen Unternehmen mit Beratungsangeboten von berufener Stelle unterstützt. Es kommt daher einem Schildbürgerstreich gleich, dass exakt zu Zeiten höchsten Bedarfes die beratende Funktion der Datenschutzbehörde für Verantwortliche abgeschafft werden soll. Während § 30 des DSG 2000 heute vorsieht, dass sich *„jedermann wegen …ihn betreffender Pflichten eines Auftraggebers oder Dienstleisters nach diesem Bundesgesetz mit einer Eingabe an die Datenschutzkommission wenden kann*“ ist eine Beratung für verantwortliche Datenverarbeiter im DSG-AnpG 2018 nicht mehr enthalten.

Diese Änderung ist auch im Lichte der DSGVO kritisch zu sehen. Die Generalklausel des Artikel 57 Abs. 1 v regelt, dass eine Aufsichtsbehörde in ihrem Hoheitsgebiet „*jede sonstige Aufgabe im Zusammenhang mit dem Schutz personenbezogener Daten erfüllen muss.*“ Auch in Erwägungsgrund 129 sind die beratenden Befugnisse ausdrücklich erwähnt, die zwar insbesondere, aber eben nicht ausschließlich den Betroffenen zu Gute kommen sollen. Wenn nun ein Mitgliedstaat bisher die Beratung Verantwortlicher als Aufgabe der Behörde betrachtet, ist die nunmehrige gänzliche Versagung nicht zu argumentieren.

Der auch von Seiten der Bundesregierung oft zitierte Grundsatz **„Beraten statt Strafen“** muss gerade in der Startphase einer einschneidenden Regulierung wie der DSGVO unbedingt Berücksichtigung finden! Die Datenschutzbehörde muss daher jedenfalls Anlaufstelle für ratsuchende Verarbeiter bzw. Datenschutz-Verantwortliche bleiben.

Internetoffensive ÖSTERREICH

3.3 Rechtsstaatliches Verfahren erforderlich

Der VwGH hat bisher bei Verhängung hoher Strafen (derzeit wohl über € 150.000,-) durch Verwaltungsbehörden eine sehr kritische Position eingenommen. Der vorliegende Gesetzesentwurf sieht vor, dass die DSB Strafen bis zu 4% des weltweiten Umsatzes, beziehungsweise € 20.000.000,-, je nachdem was höher ist, verhängen darf.

Im bisherigen Verwaltungsstrafverfahren sind die Rollen des Anklägers und des Richters nicht getrennt und der Beschuldigte muss im Verfahren mitwirken und sich damit de facto selbst belasten.

Diese Situation mag angesichts von Organstrafmandaten oder geringfügiger Strafen im Sinne der Effizienz der Verwaltung argumentierbar sein; angesichts der möglichen hohen Strafen ist diese Argumentation nicht mehr nachvollziehbar. Wir ersuchen daher den Gesetzgeber dringend folgende Punkte aufzunehmen:

- Ab einer Verwaltungsstrafe von € 150.000,- ist die Ankläger- und Richterrolle zu trennen: die DSB könnte einen Antrag auf Bestrafung beim BVwG stellen und dieses entscheidet dann. (Die Herren Professoren Potacs und Raschauer haben gezeigt, dass die DSGVO es durchaus ermöglicht, eine derartige Trennung zwischen Ankläger (DSB) und Richter (BVwG) vorzusehen.)

- Die Verschuldensvermutung, die aufgrund höchstgerichtlichen Judikatur im Bereich des § 5 VStG zu einer faktischen Erfolgshaftung geführt hat, ist (zumindest im Bereich des DSGneu) zu korrigieren, so dass er lautet wie folgt

> „**§ 5.** (1) Wenn eine Verwaltungsvorschrift über das Verschulden nicht anderes bestimmt, genügt zur Strafbarkeit fahrlässiges Verhalten. Fahrlässigkeit ist bei Zuwiderhandeln gegen ein Verbot oder bei Nichtbefolgung eines Gebotes dann ohne weiteres anzunehmen, wenn zum Tatbestand einer Verwaltungsübertretung der Eintritt eines Schadens oder einer Gefahr nicht gehört und der Täter nicht glaubhaft macht, dass ihn an der Verletzung der Verwaltungsvorschrift kein Verschulden trifft. *Dazu genügt es wenn der Täter glaubhaft macht, angemessene Vorkehrungen zur Verhinderung der Verwaltungsübertretung veranlasst zu haben. Die Bescheinigungslast entfällt zur Gänze bei Delikten mit einer Strafdrohung von mehr als [60.000,-] Euro.*“

Sollte eine Änderung des VStG nicht möglich sein, ist in § 19 DSGneu folgendes vorzusehen:

> „*(6) § 5 VStG ist mit der Maßgabe anzuwenden, dass ein Verschulden nicht vorliegt, wenn glaubhaft gemacht wird, dass angemessene Vorkehrungen zur Verhinderung der Verwaltungsübertretung veranlasst wurden. Die Bescheinigungslast entfällt zu Gänze bei Delikten ab einer Strafdrohung von mehr als € 60.000,-.*“

- An Stelle des Kumulationsprinzips ist das Absorptionsprinzip einzuführen (z.B. die mehrfache Überschreitung einer Norm durch ein technisches Gebrechen oder einen Ablauffehler sollte nur zu einer [1] Strafe führen).

- Dem Beschuldigten sind angemessene Verteidigungsrechte zu gewähren, vor allem ist sicherzustellen, dass er sich auch im Einklang mit der GRC (Art 47 Abs 2 nemo-tenetur-Prinzip) nicht selbst belasten muss.

- Beim Studium des § 11 Abs 4 DSGneu, Stichwort „Mandatsbescheid", fällt auf, dass § 11 Abs 4 DSGneu weit über die DSGVO hinausgeht. Insbesondere sieht nämlich Erwägungsgrund 129 vor, dass das betroffene Unternehmen zuvor zu hören ist (was bei einem Mandatsbescheid nicht erforderlich ist) und dass dem Verpflichteten keine überflüssige Kosten und übermäßigen Unannehmlichkeiten entstehen dürfen. Wir regen daher an § 11 Abs 4 DSGneu so zu ändern, dass er lautet wie folgt

  „(4) Liegt durch den Betrieb einer Datenverarbeitung ein *offenkundiges* wesentliche*s* unmittelbare*s* *Risiko für die Rechte und Freiheiten* der betroffenen Personen (Gefahr im Verzug) vor, so kann die Datenschutzbehörde die Weiterführung der Datenverarbeitung mit Bescheid gemäß § 57 Abs. 1 des Allgemeinen Verwaltungsverfahrensgesetzes 1991 – AVG, BGBl. Nr. 51/1991, untersagen. *Dabei dürfen nur die unter Berücksichtigung der Umstände des jeweiligen Einzelfalls und unter Abwägung der berührten Interessen erforderlichen und verhältnismäßigen Maßnahmen ergriffen werden; außerdem ist der Verantwortliche und ein allfälliger Auftragsverarbeiter, gegen den sich die nachteilige Maßnahme richtet, vorher zu hören und sind ihm gegenüber überflüssige Kosten und übermäßige Unannehmlichkeiten zu vermeiden.* Wenn dies technisch möglich, im Hinblick auf den Zweck der Datenverarbeitung sinnvoll und zur Beseitigung der Gefährdung ausreichend scheint, kann die Weiterführung auch nur teilweise untersagt werden. Ebenso kann die Datenschutzbehörde auf Antrag einer betroffenen Person eine Einschränkung der Verarbeitung nach Art. 18 DSGVO mit Bescheid gemäß § 57 Abs. 1 AVG anordnen, wenn der Verantwortliche einer diesbezüglichen Verpflichtung nicht fristgerecht nachkommt. Wird einer Untersagung nicht unverzüglich Folge geleistet, hat die Datenschutzbehörde nach Art. 83 Abs. 5 DSGVO vorzugehen."

Im Sinne der oben stehenden Erwägungen zu § 11 (4) DSGneu muss der Wortlaut des § 14 (1) DSGneu mit dem § 11 (4) DSGneu gleichgezogen werden; er sollte daher lauten wie folgt

Internetoffensive ÖSTERREICH

„**§ 14.** (1) ~~Macht der Beschwerdeführer im Rahmen einer Beschwerde eine wesentliche~~

~~Beeinträchtigung seiner schutzwürdigen Geheimhaltungsinteressen durch die Verarbeitung seiner personenbezogenen Daten glaubhaft.~~ *Liegt durch den Betrieb einer Datenverarbeitung ein offenkundiges wesentliches unmittelbares Risiko für die Rechte und Freiheiten der betroffenen Person (Gefahr in Verzug) vor, so* kann die Datenschutzbehörde nach § 11 Abs. 4 vorgehen.“

3.4 Primäre Strafbarkeit der juristischen Person

Die DSGVO hat bei den Sanktionen Unternehmen im Fokus. Im österreichischen Verwaltungsstrafrecht wird primär nicht auf das Unternehmen, sondern vielmehr auf die natürliche Person abgestellt. Diese grundsätzlich divergierenden Ansätze sind nicht leicht in Einklang zu bringen. Wir begrüßen die Anstrengungen des Gesetzgebers die Bestrafung juristischer Personen in den Vordergrund zu stellen; allerdings müssen, um dieses Ansinnen vollständig zu realisieren noch folgende Punkte geklärt werden:

Es muss klargestellt werden, dass gegen eine natürliche Person, gleichgültig ob sie Geschäftsführer, Vorstand oder verantwortlicher Beauftragter iSd VStG ist, keine Strafe verhängt werden darf, wenn für denselben Verstoß eine Verwaltungsstrafe gegen eine juristische Person möglich ist. Damit würde auch sichergestellt werden, dass es in der Regel nicht zu einer Doppelbestrafung von juristischer- und natürlicher Person kommt. § 19 Abs 3 DSGneu sollte daher lauten wie folgt:

„**§ 19.** (3) Die Datenschutzbehörde hat von der Bestrafung *einer natürlichen Person, insbesondere* 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 *oder möglich ist* und keine besonderen Umstände vorliegen, die einem Absehen von der Bestrafung entgegenstehen.“

3.5 § 17 Vertretung von betroffenen Personen

In § 17 letzter Satz DSG wird Einrichtungen, Organisationen oder Vereinigungen ohne Gewinnerzielungsabsicht auch gemäß Artikel 80 DSGVO die Berechtigung eingeräumt, Betroffene in Schadenersatzsachen zu vertreten. Da derartige Verfahren gemäß § 18 (2) in die landesgerichtliche Zuständigkeit fallen, unterliegt der belangte Verantwortliche oder Auftragsverarbeiter dem Anwaltszwang und damit einem erheblichen Kostenrisiko für Vertretungskosten. Um dieses Risiko zu begrenzen, muss zumindest der Kostenersatz für die Einrichtungen, Organisationen und Vereinigungen entfallen. Das ist möglich, da sie ja- im Unterschied zu Anwälten- ohne Gewinnerzielungsabsicht agieren.

Zudem ist die fachliche Eignung der Einrichtungen, Organisationen oder Vereinigungen sicherzustellen. Dem Wortlaut des Gesetzes ist nicht zu entnehmen ob und in welcher Form derartige Organisationen eine Zertifizierung brauchen, welche Rechtsform sie haben und welche Ausbildung die agierenden Personen nachzuweisen haben.

3.6 § 18. Haftung und Recht auf Schadenersatz

In § 18 Abs. 2 DSG wird eine örtliche Zuständigkeit für Schadenersatzklagen wegen Verletzung des Datenschutzrechtes geschaffen, die in dieser Form im allgemeinen Zivilverfahrensrecht nicht existiert.

Für Klagen auf Schadenersatz ist in erster Instanz das mit der Ausübung der Gerichtsbarkeit in Zivilrechtsangelegenheiten betraute Landesgericht zuständig, in dessen Sprengel der Kläger (Antragsteller) seinen gewöhnlichen Aufenthalt oder Sitz hat.

Die Ausdehnung auf einen allgemeinen Gerichtsstand des Klägers auch außerhalb des Konsumentenschutzrechts erscheint überschießend.

3.7 § 21 Zum Datenschutzrat

Gemäß § 21 Abs 1 Z 6 sollte neben anderen offiziellen Vertretern auch ein Mitglied der Datenschutzbeauftragten der Bundesministerien angehören. Wir würden es im Hinblick auf eine ausgewogene Zusammensetzung und somit Bereicherung des Datenschutzrates begrüßen, wenn auch ein Mitglied aus dem Kreis der privaten Datenschutzbeauftragten zu entsenden ist.

3.8 § 25 Datenverarbeitungen zu spezifischen Zwecken

Verarbeitung zum Zweck der wissenschaftlichen Forschung und Statistik

§ 25 Verarbeitung zum Zweck der wissenschaftlichen Forschung und Statistik: Die Bestimmung des § 25 ist nicht nur für die Wissenschaft und Forschung des Universitätsbereich relevant, sondern und insbesondere auch für die Wirtschaftsunternehmen in Österreich. Die Politik und die Gesellschaft haben bereits vor längerer Zeit erkannt, wie wertvoll die statistische Auswertung von Daten sein kann, um

einerseits gesellschaftliche Probleme (wie z.B. rechtzeitiges Erkennen von Krankheitsepidemien) in Angriff zu nehmen und zu lösen, aber auch zur Schaffung neuer Wirtschaftszweige (durch Monetarisierung von statistische aufbereiteten Informationen aus großen Datensammlungen - BIG Data) essentiell und wichtig sind. Big Data Anwendungen

werden in der Regel erst durch viel Ausprobieren und Forschung entwickelt und bedürfen eines entsprechenden Entwicklungsprozesses.

Die EU Kommission selbst will den freien Datenverkehr in der EU forcieren und möglich machen. Wir verweisen hierzu auf die Initiative „Europäische Datenwirtschaft: EU-Kommission stellt Konzept für Daten-Binnenmarkt vor“. Andrus Ansip, der für den digitalen Binnenmarkt zuständiger Vizepräsident wird dort zitiert mit: "Wenn unsere Datenwirtschaft Wachstum und Beschäftigung hervorbringen soll, müssen Daten genutzt werden. Dafür müssen sie allerdings verfügbar sein und analysiert werden können.
Genau das verhindert aber nun § 25 DSG

Die DSGVO sieht ein auch für diese Zwecke ausreichendes Regelungsgerüst vor. Jegliche Datenverarbeitung, die mit einem höheren Risiko verbunden ist, muss im Rahmen einer Datenschutzfolgeabschätzung extra evaluiert werden. Datensicherheitsmaßnahmen wie Pseudonymisierung werden von der DSGVO beispielhaft genannt. Dem Verarbeiter bleibt es aber im Grunde überlassen, ausreichende Datensicherheitsmaßnahmen vorzusehen, um ein Risiko gering bis Null zu halten. Die Bestimmung des § 25 Abs 1 DSG[2] würde jedoch entgegen der DSGVO genau vorgeben, wie eine Datenverarbeitung auszusehen hat. Demnach wäre die Konsequenz, dass ein Verantwortlicher für Datenanalysen einen dritten Auftragsverarbeiter heranziehen müsste und dieser „mehr können“ dürfte als der Verantwortliche selbst, denn nur für den Verantwortlichen darf eine Repersonalisierung von pseudonymisierten Daten nicht möglich sein. Es besteht auch kein Grund, Datenverarbeitungen für statistische Zwecke in Absatz zwei jedenfalls der Genehmigungspflicht durch die Datenschutzbehörde zu unterwerfen. Die DSGVO sieht hier sehr klar vor, dass dies von einer konkreten und individuellen Datenschutzfolgeabschätzung abhängt und regelt auch eine allenfalls erforderliche Vorabgenehmigung.

Zur Lösung möchten wir auf die Regelung des § 27 des Deutschen BDSG neu hinweisen, welche die DSGVO für den Bereich der wissenschaftlichen und statistischen Verarbeitung unseres Erachtens gut und richtig umgesetzt hat.

3.9 § 26 Zurverfügungstellung von Adressen zur Benachrichtigung und Befragung von betroffenen Personen

Der § 26 DSG wurde wortgleich aus dem DSG 2000 übernommen. Betrachtet man die mit der DSGVO verfolgten Intentionen (Stärkung der Eigenverantwortlichkeit, Abschätzung

[2] § 25. (1) Für Zwecke wissenschaftlicher oder statistischer Untersuchungen, die keine personenbezogenen Ergebnisse zum Ziel haben, darf der Verantwortliche der Untersuchung alle personenbezogenen Daten verarbeiten, die
1. öffentlich zugänglich sind,
2. er für andere Untersuchungen oder auch andere Zwecke zulässigerweise ermittelt hat oder
3. für ihn pseudonymisierte personenbezogene Daten sind und der Verantwortliche die Identität der betroffenen Person mit rechtlich zulässigen Mitteln nicht bestimmen kann.
(2) Bei Datenverarbeitungen für Zwecke wissenschaftlicher Forschung und Statistik, die nicht unter Abs. 1 fallen, dürfen personenbezogene Daten nur
1. gemäß besonderen gesetzlichen Vorschriften,
2. mit Einwilligung der betroffenen Person oder
3. mit Genehmigung der Datenschutzbehörde gemäß Abs. 3 verarbeitet werden.

durch die Verantwortlichen statt bürokratischer Bewilligungsverfahren) so ist ein Widerspruch feststellbar und es erscheint fraglich, ob diese zusätzliche Bewilligungspflicht mit der Datenschutzgrundverordnung vereinbar ist.

Das Instrumentarium der DSGVO sollte auch für diesen Anwendungsfall ausreichen und es besteht keine Notwendigkeit diesen Spezialfall außerhalb der europarechtlichen Vorgabe zu behandeln.

3.10 Regelung des Kindesalters im Sinne von Artikel 8 DSGVO

In Österreich dürfen gemäß dem ABGB idgF mündige Minderjährige (zwischen 14 und 18 Jahren) grundsätzlich über ihr Einkommen aus eigenem Erwerb (z.B. Lehrlingsentschädigung) und Sachen, die ihnen zur freien Verfügung überlassen worden sind (z.B. Taschengeld), frei verfügen und sich verpflichten. Wenn nun der österreichische Gesetzgeber die von der DSGVO vorgesehene Altersgrenze für die Einwilligungsfähigkeit zu Datenverarbeitungen bei 16 Jahren belässt, schafft das extreme Unsicherheit für die österreichische Wirtschaft der Informationsgesellschaft: So könnte etwa ein Jugendlicher von 14 Jahren gemäß zivilrechtlicher Regelungen wirksam einen Kaufvertrag über eine App abschließen, jedoch nicht eine damit verbundene Einwilligungserklärung zu einer Datenverarbeitung. Diese Unsicherheit wäre sehr leicht zu beseitigen, indem im DSG ausdrücklich die Altersgrenze von 14 Jahren vorgesehen wird, die somit auch konsistent mit dem Zivilrecht ist.

3.11 § 27 Freiheit der Meinungsäußerung und Informationsfreiheit

Die DSGVO bietet den Mitgliedstaaten durch Artikel 86 die Möglichkeit, den Zugang der Öffentlichkeit zu amtlichen Dokumenten auf einzelstaatlicher Ebene zu regeln. Gemäß der Richtlinie 2003/98/EG und Erwägungsgrund 154 ist davon auch die Weiterverarbeitung dieser Dokumente durch Re-User umfasst, da die Weiterverwendung von Daten, die ohne Einschränkung öffentlich zugänglich sind, auf Grundlage der EU-PSI Richtlinie und des heimischen IWG erlaubt sind.

Sowohl der Zugang zu den Daten, als auch die Weiterverwendung von öffentlichen Daten stellen ein öffentliches Interesse dar. Bezüglich des Zugangs ist dieses Interesse in Erwägungsgrund 154 festgehalten: „Der Zugang der Öffentlichkeit zu amtlichen Dokumenten kann als öffentliches Interesse betrachtet werden.“ Die PSI Richtlinie hat als erklärtes Ziel und damit öffentliches Interesse die innovative Nutzung von öffentlichen Daten durch Private: Umfassendere Möglichkeiten für die Weiterverwendung von Informationen des öffentlichen Sektors sollten u. a. die europäischen Unternehmen in die Lage versetzen, deren Potenzial zu nutzen, und zu Wirtschaftswachstum und zur Schaffung von Arbeitsplätzen beitragen.

(Erwägungsgrund 5 der Richtlinie 2003/98/EG). Die Möglichkeiten der PSI Richtlinie werden vor allem von innovativen Startups wahrgenommen.

Im Anwendungsbereich der PSI Richtlinie besteht sowohl für die Weiterverwender, als auch für die öffentliche Hand Interesse daran, dass die Daten aus öffentlichen Registern, die ohne Einschränkung zugänglich sind, im Falle der erlaubten Weiterverwendung vollständig angezeigt werden. Die vollständige und unveränderte Darstellung derartiger Datenbestände durch Re-User fördert den Transparenzgedanken öffentlicher Register. So ist beispielsweise die Veröffentlichung von Insolvenzdaten für den Gläubigerschutz unumgänglich, die Darstellung von Gewerbetreibenden in Publikationen der Wirtschaftskammer der Transparenz im Geschäftsleben und die Veröffentlichung von Abfalldeponien dem Umweltschutz förderlich.

Jeder Widerspruch von Betroffenen gemäß Artikel 21 DSGVO gegen die weitere Verarbeitung aus diesem Grund veröffentlichter Daten richtet sich daher auch gegen das öffentliche Interesse an der Transparenz. Im Falle von Artikel 21 (1) hat der Verantwortliche zwingende schutzwürdige Gründe für die Verarbeitung nachzuweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, falls er die Daten trotz Widerspruch weiterverarbeiten will. Für die Abwägung dieser Gründe gegen das Interesse der Betroffenen ist im Falle von IWG-Daten klarzustellen, dass

- Betroffene jedenfalls mit der Weiterverwendung ihrer Daten gemäß PSI Richtlinie im Sinne des Erwägungsgrundes 47 DSGVO rechnen müssen, wenn sie in öffentlich zugängliche Register eingetragen werden,
- das Geheimhaltungsinteresse praktisch nicht gegeben ist, wenn die Daten in öffentlichen Registern frei zugänglich sind,
- das öffentliche Interesse an der Transparenz gegeben ist,
- die Verarbeitung personenbezogener Daten für die Verhinderung von Betrug gemäß Erwägungsgrund 47 DSGVO ein berechtigtes Interesse ist, und
- die Vollständigkeit und Richtigkeit von Datenbanken laut Artikel 9 der Richtlinie 2008/48/EG ebenfalls ein wichtiges öffentliches Interesse darstellt.

3.12 § 29 – Verarbeitung personenbezogener Daten im Beschäftigungskontext

Wenn, wie im DSG Entwurf vorgesehen, das ArbVG (Arbeitsverfassungsgesetz) als Ganzes als relevante Vorschrift gemäß Artikel 88 DSGVO zum Datenschutzrecht im Beschäftigtenkontext erklärt wird, so ist dies jedenfalls überschießend. Das ArbVG enthält neben datenschutzrelevanten Bestimmungen im Wesentlichen kollektivarbeitsrechtliche Normen. Wenn nun alle – auch die nicht datenschutzrelevanten Bestimmungen! – der DSGVO und damit auch dem hohen Strafrahmen derselben unterworfen werden, so widerspricht dies klar den Grundsätzen der DSGVO. Wir regen daher dringend an, § 29 um einen Verweis auf § 96 und § 96a ArbVG zu ergänzen. Andernfalls ist etwa der

Nichtabschluss einer Betriebsvereinbarung trotz Vorliegen der Voraussetzungen des ArbVG per se mit dem hohen Strafrahmen der DSGVO/des DSG bedroht.

Internetoffensive ÖSTERREICH

3.13 Zur weiteren Gültigkeit von Einwilligungserklärungen

Die erläuternden Bestimmungen zu § 76 DSG regeln:

„Beruhen die Verarbeitungen auf einer Zustimmung gemäß dem DSG 2000, so ist es nicht erforderlich, dass die betroffene Person erneut ihre Einwilligung dazu erteilt, wenn die Art der bereits erteilten Zustimmung den Bedingungen der DSGVO entspricht, so dass der Verantwortliche die Verarbeitung nach dem Zeitpunkt der Anwendung der DSGVO fortsetzen kann. Dies entspricht den im Erwägungsgrund 171 der DSGVO enthaltenen Ausführungen zur „Einwilligung“ nach der Richtlinie 95/46/EG.“

Die Bedingungen für die Einwilligung werden in Art 7 DSGVO wie folgt geregelt:

1. „Beruht die Verarbeitung auf einer Einwilligung, muss der Verantwortliche nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat.

2. Erfolgt die Einwilligung der betroffenen Person durch eine schriftliche Erklärung, die noch andere Sachverhalte betrifft, so muss das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist. Teile der Erklärung sind dann nicht verbindlich, wenn sie einen Verstoß gegen diese Verordnung darstellen.

3. Die betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. Die betroffene Person wird vor Abgabe der Einwilligung hiervon in Kenntnis gesetzt. Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung sein.

4. Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, muss dem Umstand in größtmöglichem Umfang Rechnung getragen werden, ob unter anderem die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind.“

Das bedeutet, dass wenn diese Bedingungen für die Einwilligung bereits durch die Einwilligungserklärungen **vor** Anwendbarkeit der DSGVO erfüllt wurden, bedarf es keiner neuerlichen Einwilligung durch die betroffene Person.

Art 7 Abs 4 DSGVO statuiert ein sog „Koppelungsverbot“. Allerdings wird durch die Wortfolge „[…] *Umstand in größtmöglichem Umfang Rechnung getragen werden…“* großzügig formuliert. Das bedeutet, dass es jedenfalls einer Verhältnismäßigkeitsprüfung im Einzelfall bedarf, ob die Erfüllung eines Vertrags von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich

sind. Man könnte diese Regelung somit auch als ein „abgeschwächtes Koppelungsverbot“ bezeichnen.

Demgegenüber schränkt der Erwägungsgrund 43 zu Art 7 der DSGVO den Spielraum des Art 7 Abs 4 DSGVO ein und öffnet diesen gleichzeitig durch die Formulierung: „Um sicherzustellen, dass die Einwilligung freiwillig erfolgt ist, sollte diese in besonderen Fällen, wenn zwischen der betroffenen Person und dem Verantwortlichen ein klares Ungleichgewicht besteht, insbesondere wenn es sich bei dem Verantwortlichen um eine Behörde handelt, und es deshalb in Anbetracht aller Umstände in dem speziellen Fall unwahrscheinlich ist, dass die Einwilligung freiwillig gegeben wurde, keine gültige Rechtsgrundlage liefern. Die Einwilligung gilt nicht als freiwillig erteilt, wenn zu verschiedenen Verarbeitungsvorgängen von personenbezogenen Daten nicht gesondert eine Einwilligung erteilt werden kann, obwohl dies im Einzelfall angebracht ist, oder wenn die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung abhängig ist, obwohl diese Einwilligung für die Erfüllung nicht erforderlich ist“.

Der zweite Satz des Erwägungsgrunds 43 schränkt somit die pauschale Regelung des Art 7 Abs 4 DSGVO ein, da er die Freiwilligkeit verneint, wenn die Einwilligung für die Erfüllung des Vertrags nicht erforderlich ist (klassisches strenges Koppelungsverbot). Satz 1 des Erwägungsgrunds 43 öffnet jedoch die Möglichkeit einer Abwägung, ob zwischen der betroffenen Person und dem Verantwortlichen ein Ungleichgewicht besteht. In Kombination mit Art 7 Abs 4 DSGVO hat dies zur Folge, dass es einer Einzelfallprüfung bedarf, um herauszufinden, ob ein Ungleichgewicht besteht und ob im größtmöglichen Umfang abgewogen wurde, dass die Einwilligung zur Vertragserfüllung erforderlich ist.

Des Weiteren ist es Ausdruck der Privatautonomie, dass Unternehmen die Bedingungen zur Gültigkeit und Zustandekommen von Verträgen selbst festlegen können.

Die Privatautonomie steht in Österreich im Verfassungsrang (Art 5 StGG; Art 1 1. ZP EMRK). Eine Regelung, die diese einschränkt, darf nicht unverhältnismäßig sein. Hier ist besonders zu berücksichtigen, dass bei einer auf dem Markt frei verfügbaren Leistung, kein Ungleichgewicht zwischen der betroffenen Person und dem Verantwortlichen besteht, da die betroffene Person die Leistung jederzeit von einem anderen Unternehmen beziehen kann und somit die Privatautonomie unverhältnismäßig eingeschränkt wird.

Somit kann von einer Freiwilligkeit der Einwilligung der betroffenen Person ausgegangen werden, denn sie entscheidet sich wissentlich und willentlich, dass sie unter den gegebenen Bedingungen einen Vertrag mit dem Verantwortlichen abschließen möchte. Anderenfalls hätte sie nicht die Einwilligung erteilt.

Daher sollte klargestellt werden, dass die bisher gültigen Einwilligungserklärungen auch nach dem 25. Mai 2018 weiterhin gültig sind, solange sie den Bedingungen der DSGVO entsprechen und die Freiwilligkeit in oben stehender Art und Weise interpretiert wird.

Neben oben genannten Beweggründen möchten wir festhalten, dass dies auch Rechtsstaatlich geboten ist: Wenn in der Vergangenheit ein Vorgehen rechtskonform war, kann man als Unternehmen darauf vertrauen, auch künftig nicht für bisher einwandfreies Verhalten bestraft zu werden!

Dies sollte auch in den Erläuternden Bestimmungen zu § 76 festgehalten und dieser wie folgt ergänzt werden:

„Beruhen die Verarbeitungen auf einer Zustimmung gemäß dem DSG 2000, so ist es nicht erforderlich, dass die betroffene Person erneut ihre Einwilligung dazu erteilt, wenn die Art der bereits erteilten Zustimmung den Bedingungen der DSGVO entspricht, so dass der Verantwortliche die Verarbeitung nach dem Zeitpunkt der Anwendung der DSGVO fortsetzen kann. Dies entspricht den im Erwägungsgrund 171 der DSGVO enthaltenen Ausführungen zur „Einwilligung“ nach der Richtlinie 95/46/EG. *Die Bedingungen der DSGVO sehen unter anderem Freiwilligkeit vor. Eine Freiwilligkeit liegt gemäß dem Erwägungsgrund 43 zu Art 7 Abs 4 DSGVO dann nicht vor, wenn zwischen der betroffenen Person und dem Verantwortlichen ein klares Ungleichgewicht besteht, insbesondere wenn es sich bei dem Verantwortlichen um eine Behörde handelt, und es deshalb in Anbetracht aller Umstände in dem speziellen Fall unwahrscheinlich ist, dass die Einwilligung freiwillig gegeben wurde.“*

Kontaktdaten der Geschäftsstelle der IOÖ

Rotenturmstraße 17/17

A-1010 Wien

Telefon: +43 (0) 1 37 00 22 22

Fax: +43 (0) 1 907 66 00 - 111

E-Mail: office@internetoffensive.at

Internet: www.internetoffensive.at