Mag. Maximilian Schrems

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

An das
Bundeskanzleramt
Verfassungsdienst
Ballhausplatz 2
1010 Wien

Stellungnahme zum Datenschutz-Anpassungsgesetz 2018

Vorab: **Zum Gesetzgebungsverfahren**

Auch wenn den zuständigen Stellen im Bundeskanzleramt das Abhandenkommen der Regierungskoalition wohl nicht vorwerfbar ist, ist vorab anzumerken, dass die Vorgehensweise in diesem Begutachtungsverfahren äußerst besorgniserregend ist.

Obwohl es sich bei diesem Entwurf um ein heikles Ausführungsgesetz eines Grundrechtes handelt, wurde noch in der Begutachtungsfrist die Regierungsvorlage verabschiedet, nachdem die Bundesregierung vorab verlautbarte keine Regierungsvorlagen mehr zu verabschieden.

Auch eine ernsthafte parlamentarische Arbeit an diesem Entwurf scheint nicht erwartbar, wenn am Freitag, den 23. 6. die Begutachtung zu Ende geht, der Entwurf jedoch schon am Montag den 26. 6. im zuständigen Ausschuss behandelt werden soll. Es ist leider nicht zu erwarten, dass der Nationalrat die zahlreichen juristischen Problemstellen in diesem Entwurf innerhalb eines Wochenendes professionell und sachgemäß beheben kann.

Selbst für österreichische Verhältnisse scheint die gewählte Vorgehensweise einmalig. Diese Stellungnahme ist daher auch entsprechend kurz und oberflächlich gehalten, da eine ordnungsgemäße Bearbeitung der Stellungnahmen bedauerlicher Weise nicht anzunehmen ist.

Einleitende Bemerkung

Einleitend muss man anerkennten, dass der österreichische Gesetzgeber angesichts der oft unklare und mit vielen Öffnungen versehenen EU-Datenschutzgrundverordnung (DSGVO), die in vielen Bereichen im Spannungsverhältnis mit österreichischem Verfahrens- und Verfassungsrecht steht vor einer großen Herausforderung steht.

Leider macht der vorgelegte Entwurf jedoch den Eindruck viele dieser Konflikte nicht aufzulösen, sondern in vielen Teilen eine Mischung aus einer „Mindestumsetzung“ und einem „Copy/Paste“ des DSG 2000 darzustellen.

Angesichts der vielen möglichen Probleme soll sich diese Stellungnahme nur auf den Bereich der Umsetzung der DSGVO beziehen. Die Bestimmungen des 2. Abschnitts des 2. Hauptstücks und des 3. Hauptstücks sind von dieser Stellungnahme daher nicht umfasst.

Zum geplanten Beschluss mit einfacher Mehrheit

Nachdem Beobachter dieses Gesetzgebungsverfahrens davon ausgehen, dass die Bundesregierung diese Gesetz aktuell (durch Aussparung der Verfassungsbestimmungen im Entwurf) mit einfacher Mehrheit im Nationalrat beschließen will, sei generell darauf hingewiesen, dass dies in mehreren Punkten ein „hinkendes Gesetz“ erschaffen könnte und eine weiter Novelle vor dem In-Kraft-Treten der DSGVO im Jahr 2018 nötig machen wird.

Zu den einzelnen Bestimmungen

Zu Artikel 1 (Datenschutz als Bundeskompetenz):

Die Zentralisierung der Kompetenz ist jedenfalls zu Befürworten.

Das Fehlen einer solchen Bestimmung würde wohl eine teilweise Fehlende Rechtsgrundlage zu Folge haben, bzw. die Länder zur Verabschiedung von neun einzelnen „*Landes-Datenschutz-Anpassungs-Gesetzen 2018*“ zwingen - was wohl unmöglich gewollt sein kann.

Zu § 1 (Grundrecht auf Datenschutz):

Die weitere Verankerung des Grundrechts auf Datenschutz im österreichischen Verfassungsrecht scheint dringend geboten und ist klar zu befürworten.

Potentiell problematisch scheint, dass der Entwurf des § 1 DSG von **Artikel 8 GRC** strukturell und inhaltlich abweicht, was durch die doppelte Bindung im Anwendungsbereich des österreichischen und des europäischen Rechts zu Spannungen führen könnte.

Die Betroffenenrechte nach **Abs 1** scheinen unvollständig, so umfassen die Recht auf Richtigstellung und Löschung keine Verarbeitungsformen bei denen personenbezogene Daten zB nur flüchtig verarbeitet werden. Hier wäre ein genereller Anspruch auf eine Unterlassung jeglicher Verarbeitung strukturell zielführender. Eine derartige offenere und abstraktere Formulierung wäre auch mit dem System der DSVGO und des Artikel 8 GRC besser vereinbar.

Zu § 2 (Räumlicher Anwendungsbereich fehlt):

Die DSGVO erlaubt nationalen Mitgliedsstaaten bestimmte Sonderregelungen und Abweichungen. Der DSGVO fehlt – soweit ersichtlich – hierzu jedoch eine Regelung zum räumlichen Anwendungsbereich des jeweiligen mitgliedsstaatlichen Rechts in den Definitionen.

Artikel 2 der DSGVO regelt nur den Anwendungsbereich der DSGVO selbst. Ausnahmetatbestände zB nach Artikel 23 DSGVO sprechen nur davon, dass der Verantwortliche dem Recht eines Mitgliedsstaats unterliegt – nicht wie weit das Recht eines Mitgliedstaats reicht.

Der räumliche Anwendungsbereich des DSG muss daher wohl im DSG definiert werden.

> Bsp.: Wenn ein österreichisches Unternehmen zB in einer Niederlassung im EU-Ausland eine Videoüberwachung betreibt, sind § 30 ff DSG anwendbar (Sitzstaatprinzip)? ...oder gilt das jeweilige Recht am Ort der Niederlassung (Verarbeitungsort)?

Zu § 3 („Backup-Privileg"):

Auch wenn die Regelung des § 27 Abs 6 des DSG 2000 inhaltlich nicht besonders umstritten scheint, ergibt sich weder aus der Bestimmung noch aus den EB der RV die Rechtsgrundlage für diese nationale Regelung im Rahmen der DSGVO. Eine Einschränkung zB nach Artikel 23(1)(i) der DSGVO scheint zB möglich, aber ist aus dem Entwurf nicht unmittelbar erkennbar. Eine Klarstellung wäre im Sinne der Rechtssicherheit angebracht.

Zu § 4 (Verschwiegenheitspflicht des Datenschutzbeauftragten):

Es scheint sinnvoll weiter zu definieren gegenüber welchen Personen die Verschwiegenheitspflicht des Datenschutzbeauftragten nach **Abs 1** gilt. Eine generelle Verschwiegenheit (zB auch innerhalb des Unternehmens) scheint zB mit den Aufgaben nach Artikel 39 potentiell in Konflikt zu treten. Eine Klarstellung wäre im Sinne der Rechtssicherheit angebracht.

Zu § 11 (Befugnisse der Datenschutzbehörde):

Die Einschränkung in **Abs 1** von Untersuchungen auf Fälle eines „*begründeten Verdachts*" scheint nicht im Einklang mit der DSGVO zu stehen. Die DSB kann nach der DSGVO viel mehr auch strukturierte Kontrollen oder zufällige Kontrollen unternehmen.

In der Praxis scheinen zusätzlich zu den in **Abs 2** genannten Fällen insbesondere auch der „Root-Zugriff" auf Remote-Systeme und der Zugriff auf Softwarecode relevant. Die DSB arbeitet derzeit in der Praxis mitunter mit „Screenshots" von Terminal-Bildschirmen. Ein Terminal eines Mitarbeiters wird (und soll oft) nicht alle relevanten Daten anzeigen, die ein System verarbeitet. Ebenso ist zB beim Verständnis von Software ein Einblick in den Code – soweit faktisch möglich – dringend erforderlich. Eine Klarstellung hierzu scheint in Abs 2 angebracht um der DSB die Erfüllung ihrer Aufgaben nach der DSGVO (zumindest theoretisch) zu ermöglichen.

Zu § 13 (Beschränkungen im Verfahren vor der Datenschutzbehörde):

In **Abs 2, Ziffer 5** scheint das Begehren die über die Feststellung der Rechtsverletzung hinausgeht (siehe hierzu Aufzählung in Abs 5, zB Löschung) übersehen worden zu sein. Da Abs 5 diese Begehren anerkennt, scheint es sich um einen Redaktionsfehler zu handeln.

Die äußerst kurzen Fristen des **Abs 4** scheinen von der DSGVO nicht direkt gedeckt zu sein und eine reine „Kopierarbeit" aus dem DSG 2000 zu sein. Insbesondere bezüglich des europäischen Effektivitätsgrundsatzes ist wohl die Frist von drei Jahren ab einer Rechtsverletzung bedenklich, da gerade im Bereich der Datenverarbeitung Rechtsbrüche erst Jahre nach der Verarbeitung ans Tageslicht treten. Auch das Konzept des „Rechts auf Vergessenwerden" in Artikel 17 der DSGVO geht gerade von einer dynamischen Überprüfung und Änderung der Rechtmäßigkeit aus, was potentiell mit einer starren Frist von drei Jahren im Wiederspruch steht.

> Bsp.: Ich musste 2015 festgestellt, dass meine Adressdaten im Jahr 2000 illegal erfasst wurden, (als ich 13 Jahre alt war) und bis heute illegal weiterverarbeitet wurden. Der Beschwerdeweg sollte hier wohl nicht ausgeschlossen sein.

Eine Streichung der absoluten Frist von drei Jahren scheint daher angebracht.

Die Einschränkung des **Abs 5** auf private Verantwortliche scheint sich mit Artikel 58 der DSGVO nicht zu decken. Ebenso scheint die Einschränkung des Abs 5 auf gewisse Anträge des Betroffenen potentiell mit Befugnissen der DSB zB nach Artikel 58 Abs 2 Litera d) DSGVO im Spannungsverhältnis zu stehen. Eine offenere Formulierung oder eine Streichung scheint zielführender.

Der Entwurf des **Abs 6** schreibt eine höchst problematische Situation im Verfahren vor der DSB weiter fort: Die generalpräventive Wirkung der DSGVO wird durch die „*formlose Einstellung*" des Verfahrens bei *nachträglicher* Beseitigung der Rechtswidrigkeit in der Praxis unterlaufen.

Mit anderen Worten: Für Verantwortliche scheint es strategisch vorteilhaft es im Einzelfall auf ein Verfahren vor der DSB ankommen zu lassen und ggf. die Verarbeitung einzustellen anstatt sich an die Vorschriften der DSGVO zu halten.

Dies scheint nicht nur im Wiederspruch zum europarechtlichen Effektivitätsgrundsatz zu stehen, sondern in Fällen die eine Strafe nach Artikel 83 DSGVO nach sich ziehen, auch der expliziten Pflicht zur „*wirksamen und abschreckenden*" Bestrafung nach Artikel 83 Abs 1 DSGVO zu wiedersprechen. Auch wenn es verständlich ist, dass die DSB Beschwerden gerne möglichst unkompliziert einstellt, würde dies das Rechtsschutzinteresse der Betroffenen unterlaufen (zB wenn nach einer Feststellung der rechtswidrigen Verarbeitung durch die DSB auf dem zivilrechtsweg Schadenersatz verlangt wird oder ein arbeitsrechtlicher Streit von einer Frage der Datenschutzverletzung abhängig ist). Daher ist Abs 6 wohl zu streichen und die allgemeinen Regelungen des AVG anzuwenden.

Zu § 14 (Gefahr in Verzug):

Bei einer „wesentlichen Beeinträchtigung" nach **Abs 1** scheint es zielführender eine Pflicht der DSB zum Vorgehen nach § 11 Abs 4 zu verankern und die reine „kann"-Bestimmung zu ersetzen.

Zu § 17 (Vertretung von Betroffenen durch Verbände):

Der aktuell vorgeschlagene § 17 DSG scheint eine reine Wiederholung von Artikel 80 Abs 1 der DSGVO zu sein und ist wegen dessen unmittelbarer Gültigkeit wohl zu streichen.

Zu Artikel 80 Abs 2 der DSGVO (Verbandsklage):

Auch wenn die reflexartige Ablehnung von Verbandsklagen durch die WKO ein offenes Geheimnis ist, scheint der fehlende Schutz für österreichische Betroffene eine politisch nicht zu erklärende Lücke im Entwurf zum DSG zu hinterlassen:

- Österreichische Unternehmen, die am Binnenmarkt tätig sind, können weiterhin von Verbänden in anderen Mitgliedsstaaten nach Artikel 80 Abs 2 DSGVO zur Verantwortung gezogen werden, da die Zuständigkeit hier nach dem Marktortprinzip und damit nach dem Sitz des Verbandes zu beurteilen sein wird (sieh EuGH in der Rs. VKI / Henkel, C-167/00).
- Eine (finanziell schmerzhafte) „Sammelklage" mit dem Ziel des finanziellen Ausgleichs von Rechtsverletzungen kann als „Sammelklage österr. Prägung" von jedermann und als „Massen-Mandatierung" nach Artikel 80 Abs 1 DSGVO von entsprechenden Vereinen weiterhin gegen ein österreichische Unternehmen eigebracht werden.
- Die Verbandsklage nach Artikel 80 Abs 2 DSGVO dient nicht dem finanziellen Ausgleich bei Rechtsverletzungen (das Recht auf Schadenersatz ist ausgeschlossen), sondern dient primär der rechtlichen Klärung im öffentlichen Interesse (analog zu §§ 28 ff KSchG).
- Durch das Fehlen einer Verbandsklage nach Artikel 80 Abs 2 DSGVO sind potentielle Kläger wie der VKI oder die Arbeiterkammer wohl in der Praxis sogar gezwungen auf schadenersatzrechtliche „Sammelklagen" auszuweichen, da zB Unterlassungsansprüche oder Auskunftsansprüche mitunter höchstpersönlich sein könnten.
- Gleichzeitig sind österreichische Unternehmen *de facto* nur zu einem minimalen Teil ein potentielles Ziel von Datenschutz-Verbandsklagen, da es in Österreich fast keine Industrie im Bereich der gezielten Verarbeitung von personenbezogenen Daten gibt. Ein Ziel von Klagen nach Artikel 80 Abs 2 DSGVO wären in der Praxis wohl primär Unternehmen in Drittstaaten (insbesondere den USA) und teilweise im EU-Ausland.
- Folglich wird mit dem Entwurf primär der unlautere Wettbewerb durch weniger rechtstreue Unternehmen am heimischen Markt gestützt, nicht die heimische Wirtschaft.

Zusammenfassend verhindert der Entwurf daher ein wichtiges Werkzeug für die rechtliche Klärung in Fällen von potentiellen Datenschutzverletzungen, ohne die Befürchtungen der österreichischen Wirtschaftsvertreter lösen zu können. Hier wird maximal eine „Scheinlösung" suggeriert, die in der Praxis nicht aufrechtzuerhalten ist.

Es ist politisch auch nicht erklärlich warum österreichischen Betroffenen gegenüber Unternehmen im EU-Ausland und Drittstaaten im Entwurf dieses Recht vorenthalten wird, wenn dies zB in der Bundesrepublik Deutschland heute schon geltendes Recht ist und auch gegen heimische Unternehmen, die am Binnenmarkt teilnehmen, Anwendung finden wird.

Mit anderen Worten: Der Entwurf kann nicht verhindern, dass heimische Unternehmen Ziel einer Verbandsklage im Binnenmarkt werden, der Entwurf könnte aber verhindern, das österreichische Betroffene weniger Schutz erhalten als Betroffene auf der anderen Seite des Walserbergs – diesen Schutz scheint der Entwurf absichtlich nicht zu bieten.

Zu § 18 (Zivilrechtliche Durchsetzung):

Das Recht auf materiellen und immateriellen Schadenersatz im ersten Satz des **Abs 1** ergibt sich direkt aus der DSGVO und ist daher wohl nicht besonders zu wiederholen. Der weitere Verweis auf das bürgerliche Recht scheint jedoch sinnvoll, da es zumindest Teilweise Lücken in der Schadenersatzregelung der DSGVO gibt.

Konzeptionell vollkommen misslungen scheint **Abs 2**, da dieser lediglich Klagen auf Schadenersatz erfasst. Die DSGVO geht ausdrücklich von einer parallelen Möglichkeit der Beschwerde bei der DSB und einer Klagemöglichkeit vor Zivilgerichten vor (so zB ausdrücklich Artikel 79 DSGVO). Im vollen Bewusstsein, dass dies auf heftigen Wiederstand der Bundesregierung bei der Verhandlung der DSGVO gestoßen ist, scheint diese Schlacht geschlagen und wurde bereits in Brüssel verloren. Äußerst verwunderlich scheint daher die Einschränkung der Zuständigkeitsbestimmung allein auf Schadenersatzklagen.

Da man dem Entwurf wohl nicht unterstellen kann, dass er Artikel 79 „*wegignorieren*" will, bleibt nur der Schluss zu, dass andere Klagen (zB auf Auskunft, Löschung, Richtigstellung, etc) ebenso von Abs 2 umfasst sein müsste – will man eine „Zersplitterung" von einheitlichen Klagen zwischen Gerichten erster Instanz, Arbeitsgerichten oder den Bezirksgerichten verhindern.

Mangels einer Regelung zu anderen Klagen nach Artikel 79 Abs 1 DSGVO sind nämlich für alle anderen Ansprüche nach der DSGVO nach dem aktuellen Entwurf die allgemeinen Regelungen der JN, der ZPO, des Artikel 79 Abs 2 DSGVO und der EuGVVO anwendbar.

Der Entwurf übersieht auch, dass eine datenschutzrechtlicher Anspruch mitunter mit zivilrechtlichen (zB nach § 16 ABGB) oder arbeitsrechtlichen Ansprüchen gemeinsam in einer Klage vorgebracht wird. Eine „*Klage auf Schadenersatz*" in der vom Entwurf erdachten Reinform, ist praxisfremd. Hier scheint ein entsprechender Normenkonflikt vorprogrammiert.

Zusammenfassend ist Abs 2 wohl entweder vollkommen zu streichen, oder aber durch eine Regelung zu ersetzen, die jegliche Klage in der Ansprüche nach der DSGVO oder dem DSG geltend gemacht werden, den Gerichten erster Instanz zuweist.

Zu § 19 (Strafbestimmungen)

Das Spannungsverhältnis zwischen dem Verwaltungsstrafsystem der DSVGO (zB mit Strafen von € 20 Mio gegen juristische Personen) und dem österreichischen Recht ist evident.

Vollkommen unklar scheint das Zusammenspiel der Verwaltungsstrafen der DSGVO und Strafen nach dem österreichischen Strafrecht. Ein Vorrang des Strafrechts scheint bei „*Trivialdelikten*" die Strafsystematik der DSGVO mit bis zu € 20 Mio zu unterlaufen. Gleichzeitig scheint eine parallele gerichtliche Strafbarkeit und Verwaltungsstrafbarkeit – angesichts der Strafhöhen in der DSGVO – im Spannungsverhältnis mit dem Doppelbestrafungsverbot zu stehen.

Es mag in einigen Bereichen der „Quadratur des Kreises" zu bedürfen um diese Situation aufzulösen – leider scheint der Entwurf diese Aufgabe aber nicht zu lösen:

- Die Einschränkung des **Abs 1** scheinen – zumindest auf den ersten Blick – keine Deckung in der DSGVO zu finden. So sind durchaus Konstellationen vorstellbar, die eine Strafbarkeit nach der DSGVO bringen, jedoch nicht unter eine der drei Fälle des Abs 1 fallen.

- Ebenso scheint die Einschränkung in **Abs 2** problematisch: So entfällt eine Verwaltungsstrafe nach der DSGVO, wenn die Tat auch zB nach dem StGB strafbar ist. Dabei ist zB an Delikte gegen die Privatsphäre (§§ 118 ff StGB) zu denken. In der Konsequenz könnte nach Abs 2 allein die Strafbarkeit zB nach § 119 StGB („Verletzung des Telekommunikationsgeheimnis“) die Verwaltungsstrafe nach Artikel 83 DSGVO überlagern. Da § 119 StGB ein Ermächtigungsdelikt ist und eine maximale Freiheitsstrafe von 6 Monaten vorsieht, könnte damit die europarechtliche Strafe nach der DSGVO „ausgehebelt“ werden: Im Extremfall bleibt von € 20 Mio. Verwaltungsstrafe nach DSGVO nur noch eine Diversion nach der StPO übrig – was wohl klar europarechtswidrig wäre.
- Vollkommen unklar ist der Unterschied zwischen **Abs 1 und Abs 2**: Die Regelung des Abs 1 sieht nicht vorsieht, dass die Verwaltungsstrafe nach der DSGVO gegenüber einer gerichtlichen Strafe nach österreichischem Strafrecht zurücktritt, Abs 2 tut genau das. Die Regelung des Abs 1 sieht also eine Parallelbestrafung vor, Abs 2 eine Alternativbestrafung.
- Nach **Abs 3** scheint der Entwurf wiederum von einer parallelen Verwaltungsstrafbarkeit des Verantwortlichen und der Strafbarkeit der Vertreter und Mitarbeiter auszugehen. Dies scheint wiederrum nicht direkt im Sinne der DSGVO zu sein. Die DSGVO scheint – zumindest auf den ersten Blick – von einer Strafbarkeit des „Verantwortlichen“ (also des Unternehmers oder der juristischen Person selbst – nicht des Verantwortlichen oder des Mitarbeiters) auszugehen.

Zu § 30 ff (Videoüberwachung)

Es wäre zwar zu begrüßen wenn der österreichische Gesetzgeber spezielle Fälle der Datenverarbeitung weiter definieren könnte, leider ist aber in der DSGVO gerade zum hier relevanten Punkt der „*berechtigten Interessen*“ nach Artikel 6 Abs 1 Litera f der DSGVO keine Öffnungsklausel vorhanden. Der vorgesehene 6. Abschnitt ist jedoch nichts anderes als eine nationale Ausführung der Abwägung nach dieser Bestimmung in der DSGVO und daher wohl in dieser Form europarechtswidrig. Auch wenn politisch die genauere Definition derartiger Verarbeitungsschritte sicherlich sinnvoll ist, wäre daher eine entsprechende rechtlich Grundlage in der DSGVO zu benennen, was der Entwurf verabsäumt.

Würde der Abschnitt auf Fälle der „Videoüberwachung“ zur Verhinderung und Aufklärung von Straftaten eingeschränkt, könnte ggf. Artikel 10 der DSGVO (Verarbeitung von strafrechtlichen Daten durch Private) als Rechtsgrundlage genutzt werden.

Inhaltlich schein der Entwurf sowohl europarechtlich als auch verfassungsrechtlich höchst bedenklich da die Regelung keinen „Anlassfall“ (siehe § 50a Abs 2 DSG 2000) für eine Auswertung von gespeicherten Videoüberwachungsdaten mehr vorsieht. Die gesamte grundrechtliche Logik der Verhältnismäßigkeit einer „*Video-Vorratsdatenspeicherung*“ liegt aber gerade darin, dass ausschließlich in einem Anlassfall (zB bei einem Diebstahl) das Recht auf Datenschutz von unbeteiligten Dritten durch das Interesse des Verantwortlichen aufgewogen wird – nicht jedoch außerhalb diese Anlassfalls, wo keinerlei rechtlich geschütztes Interesse des Verantwortlichen für eine Datenauswertung besteht.

Der 6. Abschnitt bedürfte daher einer dringenden Überarbeitung im Hinblick auf die Rechtsgrundlage im Rahmen der DSGVO und der Einschränkung der Auswertung auf Anlassfälle.

Zu § 70 (Gerichtliche Strafbestimmung)

Entsprechend den Ausführungen zu § 19 des Entwurfs oben scheint insbesondere der Vorschlag des § 70 einen Konflikt mit den Verwaltungsstrafen nach Artikel 83 DSGVO geradezu heraufzubeschwören. Eine Streichung von § 70 wäre wohl anzudenken, da sich die Vorgängerbestimmung im DSG als wenig genutzt herausgestellt hat.

Sonstige Anregungen

- ***Strafbarkeit und Durchsetzung bei öffentlichen Stellen***

Die Durchsetzung der DSGVO im öffentlichen Bereich ergibt sich – zumindest bei oberflächlicher Betrachtung – nicht unmittelbar. Öffentliche Stellen sollen weder nach Artikel 83 DSGVO strafbar sein, noch kann die DSB nach § 13 Abs 5 des Entwurfs einer öffentlichen Stelle die Verarbeitung untersagen. Möglich scheint eine Strafbarkeit des Entscheidungsträgers.

Ob damit der Entwurf eine Effektive Rechtsdurchsetzung im öffentlichen Bereich sicherstellt, scheint zumindest fraglich.

- ***Option: Einwilligung von Jugendlichen mit 14 Jahren, statt 16 Jahren***

Die DSGVO sieht generell eine Altersgrenze für eine gültige Einwilligung ab 16 Jahren vor. Artikel 8 Abs 1 DSGVO erlaubt es den Mitgliedsstaaten jedoch davon abzugehen.

Angesichts der in der österreichischen Rechtsordnung durchgehenden Definition von mündigen Minderjährigen mit einem Alter von 14 Jahren, wäre es wohl systemwidrig im Bereich des Datenschutzes ein, der Rechtsordnung sonst nicht bekanntes, Alter von 16 Jahren zu nutzen.

Es wäre daher zu befürworten wenn das DSG von der Option in Artikel 8 Abs 2 der DSGVO Gebrauch macht und das Alter für die Einwilligung auf 14 Jahre senkt.

Wien, am 22. 6. 2017