



Bundeskanzleramt-Verfassungsdienst
Präsidium des Nationalrates

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

Bundesrechenzentrum GmbH
Hintere Zollamtsstraße 4, 1030 Wien
Telefon: +43 (0)1 711 23
www.brz.gv.at

Mag. Barbara Schmidt-Bridge
+43 1 71123-883345
Barbara.Schmidt-Bridge@brz.gv.at
Dipl.-Ing Reinhard Fiegl, MBA MSc
+43 1 71123-882574
Reinhard.Fiegl@brz.gv.at

Wien, am 23. Juni 2017

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

Sehr geehrte Damen und Herren,

die BRZ GmbH, als zentraler IT-Dienstleister und E-Government-Partner der öffentlichen Verwaltung, erlaubt sich im Rahmen der öffentlichen Konsultation des Bundeskanzleramtes 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:

Ad § 1 „Grundrecht auf Datenschutz“:

§ 1 Abs. 1:

Zentraler Anknüpfungspunkt des Rechtes auf Datenschutz ist das Recht auf Geheimhaltung personenbezogener Daten im Rahmen eines schutzwürdigen Interesses. Der vorgeschlagene § 1 des Datenschutzgesetzes (DSG) enthält, wie auch wie der geltende § 1 DSG 2000, eine Verfassungsbestimmung, in der dieses Grundrecht, abgeleitet von Art. 8 Europäischer Grundrechtecharta und weiteres Art. 8 der Europäischen Menschenrechtskonvention, konkret ausgestaltet wurde. Das dem zugrunde liegende Recht auf Schutz personenbezogener Daten regelt das jedermann zustehende Recht, dass seine personenbezogenen Daten nur unter bestimmten Voraussetzungen verarbeitet werden und es regelt weiters, dass die betroffene Person Auskunft über die sie



betreffenden erhobenen Daten erlangen können muss und gegebenenfalls die Berichtigung der Daten erwirken kann. Die Löschung unzulässig verarbeiteter Daten ist hiervon aber nicht umfasst. Das im vorgeschlagenen Wortlaut des in den Verfassungsrang zu hebenden § 1 Abs. 1 DSGVO enthaltene Recht auf Löschung dehnt den bisher gewährten grundrechtlichen Schutz somit aus.

Es stellt sich zudem die Frage, ob ein absolutes Recht auf Löschung mit der Rechtsprechung des Verfassungsgerichtshofes vereinbar ist. § 28 Abs. 2 DSGVO 2000 wurde als verfassungswidrig aufgehoben, da ohne Begründung des Begehrens ein generelles Widerspruchsrecht des Betroffenen zu einer fehlenden Interessenabwägung führen würde, wenn nicht auf die konkreten Umstände des Einzelfalles abgestellt wird (vgl VfGH 08.10.2015, G 264/2015).

Weiters sollte im vorgeschlagenen DSGVO noch klargestellt werden, was unter „löschen“ im Detail verstanden wird. Die Löschung von Daten stellt Verantwortliche und Auftragsverarbeiter in der Praxis nämlich vor größte Schwierigkeiten, da es technisch in vielen Fällen nicht möglich ist, einzelne Datensätze aus einem Gesamtdatensatz zwecks Lösungsverpflichtung zu extrahieren. Ohne Zweifel kann bei neu zu entwickelnden Applikationen dem Umstand der Datenlöschungsverpflichtung durch ein entsprechendes Applikationsdesign Rechnung getragen werden. Bei vorhandenen Datenverarbeitungen ist dies rückwirkend nicht möglich.

§ 1 Abs. 2:

Der Gesetzgeber sieht im vorliegenden Gesetzesentwurf taxativ aufgezählte Tatbestände vor, in denen Beschränkungen des Grundrechtes auf Datenschutz ermöglicht werden. Diese finden nicht vollständig in Art. 6 DSGVO Deckung. Damit wird eine Rechtsunsicherheit geschaffen, die zu vermeiden wäre.

Ad § 3 „Durchführungsbestimmung“:

Es wurde generell nicht auf Besonderheiten der Löschpflicht von einzelnen Einträgen in Protokolldateien und von Protokolldateien als Ganzes näher eingegangen. Es liegt im Interesse eines Verantwortlichen und Auftragsverarbeiters, Protokolldateien als wichtiges Werkzeug für die Zulässigkeit einer Verarbeitung heranzuziehen, auch um im Nachhinein Überprüfungen und Nachvollziehbarkeit vornehmen und gewährleisten zu können. Mit einer Löschung von Daten eines Betroffenen aus Verarbeitungstätigkeiten und der damit verbundenen Berücksichtigung der Löschung einzelner Einträge in Protokolldateien, aber auch durch eine zu gering bemessene Lösungsfrist von Protokolldateien als Ganzes, wäre dies nicht mehr möglich.

Eine Klarstellung, wie seitens des Verantwortlichen und Auftragsverarbeiters mit Protokolldaten eines Betroffenen umgegangen werden soll, und eine zeitlich klar definierte Lösungsfrist von Protokolldateien als Ganzes analog wie in § 14 Abs. 5 DSGVO 2000 vorgesehen, würde einen wichtigen Beitrag zu Rechtssicherheit darstellen.



Bedauerlicherweise wurde im vorliegenden Entwurf zum DSG nicht die durch Art. 17 DSGVO eröffnete Möglichkeit genutzt, auf die Besonderheiten der Löschungspflicht in Archivsystemen näher einzugehen. Laut Art. 17 Abs. 3 lit b DSGVO besteht nämlich die Möglichkeit einer technische Umsetzung einer vollständigen Löschung, die den Ansatz vertritt, dass nicht zwingend in Form einer physikalischen Löschung sondern einer logischen Löschung vorgegangen werden kann. Eine Klarstellung wie mit einer Löschung in Archivsystemen umzugehen ist, wenn diese vor einer ursprünglich eingestellten Behaltdauer durch beispielsweise Ausübung eines Betroffenenrechts auszuführen ist, schafft Rechtssicherheit.

Ad § 5 iVm § 15 : „öffentlicher Bereich“:

Eine klare Trennung von öffentlichen und privaten Bereich ist dem vorliegenden Entwurf des Datenschutzgesetzes nicht zu entnehmen; es ist auch unklar, ob mit dem Begriff „öffentliche Stelle“ der Begriff des „öffentlichen Bereichs“ gleichgesetzt werden kann. Da an diese Begriffe weitreichende Rechtsfolgen geknüpft sind, wie beispielsweise das Erfordernis eines Datenschutzbeauftragten oder die Verhängungen von Geldbußen, ist eine eindeutige Begriffsdefinition dienlich, um hier hinreichend Rechtssicherheit zu schaffen.

Ad § 11 „Befugnisse der Datenschutzbehörde“:

§ 11 Abs. 4 iVm § 34 „Anwendungsbereich“:

Generell gesprochen, erscheinen die im vorgeschlagenen § 11 Abs. 4 DSG genannten Möglichkeiten der Datenschutzbehörde, in den operativen Betrieb von Datenanwendungen eingreifen zu können, sehr weitreichend und sollten Eingriffe wie Untersagung der Weiterführung nur bei Gefahr in Verzug für die Rechte und Freiheiten von betroffenen Personen unter Berücksichtigung der in Erwägungsrund 129 der DSGVO genannten Erfordernisse der Anhörung der Person, gegen die sich die Maßnahme richtet, Eignung, der Erforderlichkeit sowie Verhältnismäßigkeit unter Berücksichtigung des Einzelfalles angewandt werden. Es sollte in jedem Fall eine Interessenabwägung auch zum Schutz der Verantwortlichen und gegebenenfalls Auftraggeber stattfinden, wobei klarzustellen ist, dass ein Schadenseintritt unmittelbar droht und nicht bloß eine Gefährdung von schutzwürdigen Geheimhaltungsinteressen der betroffenen Person vorliegt. Diese Interessenabwägung könnte ähnlich wie im Exekutionsverfahren bei Erlassung einer Einstweiligen Verfügung stattfinden, wobei für den Rechtsbehelf gegen die Entscheidung der Datenschutzbehörde die Möglichkeit der aufschiebenden Wirkung unerlässlich erscheint, da andernfalls für Unternehmen eine existentielle Bedrohung eintreten könnte.

Weiters scheint es in Zeiten, in denen Datenverarbeitungen örtlich nicht mehr unmittelbar eingrenzbar sind (wie etwa bei virtualisierten Systemen, die kurzfristig ihre geografischen Standorte wechseln können oder bei Cloud Lösungen, bei denen eine geografische Verortung von Daten ebenfalls schwierig ist) fragwürdig, ob das Betreten von Räumen und die Anfertigung von Kopien zweckmäßig sind.



§ 11 Abs. 5 „Verwaltungsstrafbestimmung“:

Die Datenschutzbehörde wird ermächtigt, im Rahmen ihrer Zuständigkeit neben Abhilfebefugnissen gemäß Art. 58 Abs. 2 DSGVO nunmehr auch Geldbußen gegenüber natürlichen und juristischen Personen zu verhängen, die im Lichte des Art. 83 DSGVO durchaus wirksam, verhältnismäßig und abschreckend sein sollten, im Einzelfall bis zu EUR 20 Millionen bzw. 4 % des gesamten weltweiten erzielten Jahresumsatzes des vorangegangene Geschäftsjahres betragen können.

In Anbetracht dieser sehr hohen Strafandrohung scheint zweifelhaft, ob die Verhängung solcher Strafen durch die Datenschutzbehörde zulässig gestaltet ist. Die DSGVO geht grundsätzlich davon aus, dass Verwaltungsbehörden diese Geldbußen verhängen, sie sieht aber auch in Art. 89 Abs. 3 DSGVO die Öffnungsklausel vor, dass Mitgliedstaaten, deren Verwaltungsrechtsregelungen keine entsprechende Ermächtigung zur Verhängung von Geldbußen haben, Regelungen vorsehen können, in denen die nationale Aufsichtsbehörde die Ermittlungen einleitet und vornimmt und in der Folge ein nationales Gericht über die Verhängung von Geldbußen abspricht.

Weiters wird noch angemerkt, dass nicht alle Verwaltungsstrafbestimmungen des Entwurfs aufgrund des Rechts der Europäischen Union erforderlich sind.

Ad § 19 „Allgemeine Bedingungen für die Verhängung von Geldbußen“:

Im vorgeschlagenen § 19 Abs. 5 DSG der Begriff „öffentliche Stelle“ eingeführt, ohne nähere Definition oder Erläuterung. Aufgrund der Konsequenzen des vorgeschlagenen § 19 Abs. 5 DSG wird angeregt, den Begriff der „öffentlichen Stelle“ im DSG zu definieren, um Rechtsunsicherheiten zu vermeiden. Durch die Erwägungen der DSGVO (Erwägungsgrund 154) wird zwar klar, dass der Begriff iSd Richtlinie 2003/98/EG des Europäischen Parlaments und des Rates vom 17. November 2003 über die Weiterverwendung von Informationen des öffentlichen Sektors zu verstehen ist. Damit wird auch die Einheitlichkeit der nationalen Rechtsordnung gewährleistet, nachdem diese Begriffsdefinition auch der Definition der „öffentlichen Stelle“ des Informationsweiterverwendungsgesetz entspricht und somit die „öffentliche Stelle“ einen einheitlichen Begriffsinhalt hat. Eine Klarstellung wäre dennoch dienlich.

Ad § 30 bis § 33 „Bildverarbeitung“:

Es ist unklar, wie das Verhältnis einer von der seinerzeit nach der Standard- und Muster-Verordnung 2004 umfassten Videoüberwachung zu den Regelungen der DSGVO und des nunmehr vorliegenden Entwurfs des DSG zu werten ist.

Ad § 50 „Protokollierung“:

Zur Nachvollziehbarkeit von Verarbeitungsvorgängen, zur Überprüfung der Rechtmäßigkeit der Datenverarbeitung und zur Eigenüberwachung ist die in § 50 angeführte



Protokollierung ein wichtiges Nachweisinstrument. Eine Festlegung der Aufbewahrungsdauer von Protokolldaten analog zum geltenden § 14 Abs. 5 DSG 2000 wäre wünschenswert, sowohl im Interesse des Betroffenen, als auch der Aufsichtsbehörde und des Verantwortlichen.

Ad § 52 „Datenschutz-Folgenabschätzung“ iVm §71ff „Schlussbestimmungen“:

Es ist im vorgeschlagenen DSG leider keine Klarstellung enthalten, wie hinsichtlich der Erstellung einer Datenschutz-Folgeabschätzung für eine bereits gemeldete oder auf einer Standardanwendung beruhenden Datenverarbeitung vorgegangen werden soll. Wünschenswert wäre hier eine Regelung, die Klarheit schafft.

Die Datenschutzbehörde ist jedenfalls angehalten, wie im Art. 35 Abs. 4 und Abs. 5 DSGVO sowie im vorgeschlagenen § 10 Abs. 2 DSG vorgesehen, zeitnah eine Liste der Verarbeitungsvorgänge zur Verfügung stellen, für die Datenschutz-Folgenabschätzungen entweder gar nicht oder jedenfalls durchzuführen wären. Es könnte dabei auf bereits existierende Standardanwendungen Rücksicht genommen werden sowie könnten bereits durch die Aufsichtsbehörde unter dem Regime des DSG 2000 genehmigten Verarbeitungstätigkeiten umfasst sein.

Ad § 76 Abs. 4 und 5 „Übergangs- und Schlussbestimmungen“:

In diesen Übergangsbestimmungen wird geregelt, dass zum geltenden DSG 2000 anhängige Verfahren nach den Bestimmungen des vorliegenden Entwurfes fortzuführen sind und weiters, dass Verletzungen des DSG 2000, die zum Zeitpunkt des Inkrafttretens des vorgeschlagenen DSG noch nicht anhängig waren, nach der Rechtslage nach Inkrafttreten des vorgeschlagenen DSG zu beurteilen sind. In den erläuternden Bemerkungen zum vorgeschlagenen § 76 DSG findet sich hingegen die Anmerkung, dass ein strafbarer Tatbestand, der vor dem Inkrafttreten dieses Bundesgesetzes verwirklicht wurde, nach jener Rechtslage zu beurteilen ist, die für den Täter in ihrer Gesamtauswirkung günstiger ist (vgl auch § 1 Abs. 2 VStG). Betrachtet man die erhöhte Strafandrohung des vorgeschlagenen DSG wird von einer günstigeren Rechtslage für den Täter nach in Kraft treten des vorgeschlagenen DSG regelmäßig nicht die Rede sein können. Eine Überarbeitung des Gesetzestextes ist wohl dienlich.



Die BRZ GmbH bedankt sich im Voraus für die Berücksichtigung im Rahmen des Gesetzgebungsprozesses und steht für Rückfragen jederzeit gerne zur Verfügung.

Mit freundlichen Grüßen

Mag. Philipp Abbrederis
Leiter Einkauf und Recht