Hauptverband der
österreichischen
Sozialversicherungsträger

Bundeskanzleramt

Präsidium des **Nationalrates**

T + 43 (0) 1 / 71132-1211
recht.allgemein@sozialversicherung.at
Zl. REP-43.00/17/0130 Ht

Wien, 19. Juni 2017

Betreff: Datenschutz-Anpassungsgesetz 2018

Bezug: Ihr E-Mail vom 12. Mai 2017,
GZ: BKA-810.026/0019-V/3/2017

Sehr geehrte Damen und Herren,

der Hauptverband der österreichischen Sozialversicherungsträger nimmt wie folgt Stellung:

Aus unserer Sicht könnte bzw. sollte von den im Rahmen der EU-Datenschutz-Grundverordnung (DSGVO) eingeräumten Gestaltungsmöglichkeiten verstärkt Gebrauch gemacht werden.

Die in der DSGVO enthaltenen erheblichen Strafdrohungen sollten klarer, übersichtlicher und leichter nachvollziehbar geregelt werden. Auf eine Publikation des Deutschen Forschungsinstituts für öffentliche Verwaltung wird hingewiesen.[1]

Zu den einzelnen Bestimmungen wird Folgendes angemerkt.

Zu § 1 DSG

Die Erläuterungen weisen auf die Notwendigkeit der Verankerung von Speicherfristen in den Materiengesetzen hin. Was als solches Gesetz gilt, wird nicht behandelt und sollte in den Erläuterungen definiert werden. Bis dahin ist im Rahmen der österreichischen Rechtsordnung davon auszugehen, dass nicht nur formelle, sondern auch materielle Gesetze dafür ausreichen. Unserer Ansicht ist nach derzeitiger Rechtslage eine Verankerung in den Weisungen für die Rechnungslegung und Rechnungsführung bei den Sozialversicherungsträgern und dem Hauptverband (Rechnungsvorschriften RV, § 444 Abs. 6 ASVG) oder in der

[1] Die Datenschutz-Grundverordnung und das nationale Recht: Erste Überlegungen zum innerstaatlichen Regelungsbedarf; http://www.foev-speyer.de/files/de/downloads/Kuehling_Martini_et_al_Die_DSGVO_und_das_nationale_Recht_2016.pdf

Wien 3 · Kundmanngasse 21
1031 Wien · Postfach 600
www.hauptverband.at
DVR 0024279

Hauptverband der
österreichischen
Sozialversicherungsträger

Datenschutzverordnung für die gesetzliche Sozialversicherung (SV-DSV, § 31 Abs. 12 ASVG) ausreichend.

Dies wäre auch in jenen Angelegenheiten ausreichend, die im übertragenen Wirkungsbereich zu vollziehen sind. Falls nicht, müsste in den entsprechenden Materiengesetzen (bspw. Bundespflegegeldgesetz, Kinderbetreuungsgeldgesetz, Familienzeitbonusgesetz) eine Speicherfrist verankert werden, welche mit den einschlägigen Regeln des Sozialversicherungsrechts korreliert.

Zu § 1 Abs. 2 DSG

Der erste Satz ist missverständlich (worauf bezieht sich die Erwähnung der gesetzlichen Grundlage?) und sollte unter gleichzeitiger Korrektur des Schreibfehlers wie folgt formuliert werden:

„*Beschränkungen sind nur mit Einwilligung der betroffenen Person, in* ***deren*** *lebenswichtigen Interesse,* ***im öffentlichen Interesse aufgrund einer gesetzlichen Grundlage*** *oder im überwiegenden berechtigten Interesse eines anderen zulässig.*"

In diesem Zusammenhang gehen wir davon aus, dass bereits vorhandene Einwilligungen (bei gleichem Datenbestand) auch weiterhin gelten und nicht wegen Änderung der Rechtslage neu eingeholt werden müssen.

Zu § 5 Abs. 1 DSG

Laut Abs. 1 hat „das oberste Organ" das Recht, sich über Gegenstände der Geschäftsführung beim Datenschutzbeauftragten im öffentlichen Bereich zu unterrichten.

Auch die von den einzelnen Sozialversicherungsträgern zu benennenden Datenschutzbeauftragten sind dem „öffentlichen Bereich" zuzuordnen (siehe die Erläuterungen). Es sollte klargestellt werden, dass sich die Berichterstattungspflicht gegenüber dem „obersten Organ" lediglich auf die Datenschutzbeauftragten der Behörden der allgemeinen staatlichen Verwaltung bezieht und die *Berichtspflicht bei anderen juristischen Personen* des öffentlichen Bereichs nach wie vor deren geschäftsführende Organe, nicht jedoch die Datenschutzbeauftragten betrifft.

Zu § 5 Abs. 3 DSG

Für juristische Personen wie die Sozialversicherungsträger, die im übertragenen Wirkungsbereich Gesetze vollziehen (bspw. Bundespflegegeldgesetz, Kinderbetreuungsgeldgesetz, Familienzeitbonusgesetz), sollte klargestellt werden, welche

Wien 3 · Kundmanngasse 21
1031 Wien · Postfach 600
www.hauptverband.at
DVR 0024279

Hauptverband der
österreichischen
Sozialversicherungsträger

Aufgaben von welchem Datenschutzbeauftragten (Datenschutzbeauftragter des Sozialversicherungsträgers oder des Ministeriums) betreut werden und ob ein regelmäßiger Erfahrungsaustausch auch mit den Datenschutzbeauftragten der Sozialversicherungsträger erforderlich ist.

Zu §§ 11 Abs. 4, 14 Abs. 1, 26 Abs. 2 und 4, 70, 76 Abs. 2 DSG

Die Wortfolge „schutzwürdige (Geheimhaltungs-)Interessen" sollte entsprechend der Terminologie der DSGVO durchgängig durch „berechtigte Interessen" ersetzt werden.

Zu § 13 Abs. 9 DSG

Für die vorgesehene Beiziehung von Amtssachverständigen durch die Datenschutzbehörde wäre Regelung hinsichtlich der Kostentragung zu ergänzen. Es sollte eine Klarstellung erfolgen, dass die Datenschutzbehörde in diesem Fall die Kosten zu tragen hat.

Zu § 14 Abs. 2 DSG

Nach dem derzeitigen § 31a Abs. 3 DSG 2000 muss ein Bestreitungsvermerk vom Beschwerdegegner dann nicht angebracht werden, wenn er die Richtigkeit der Daten begründen und belegen kann. Diese Regelung sollte beibehalten werden.

Zu § 19 Abs. 3 DSG

Generell wäre klarzustellen, ob eine „Geldbuße" eine Verwaltungsstrafe ist oder ein Rechtsfolge eigener Art. Der Verwaltungsgerichtshof hat bisher entschieden, dass eine Geldbuße (im Anlassfall: nach § 334 Abs. 7 BVergG 2006) keine Verwaltungsstrafe ist, sondern damit ein neues Sanktionssystem normiert ist (siehe VwGH 16. 12. 2015, Ro 2014/04/0065 und 11. 11. 2015, Ra 2015/04/0073).

Abs. 5 über die Zulässigkeit der Verhängung von Geldbußen entspricht der geltenden Rechtslage des Verwaltungsrechts (§ 5 Abs. 4 VerwVollstreckungsG – keine Vollstreckung gegen Körperschaften des öffentlichen Rechts), entsprechende Maßnahmen werden effizienter durch die jeweiligen Aufsichtsbehörden (vgl. deren Rechte nach § 449 Abs. 1 letzter Satz sowie § 451 ASVG) durchgesetzt werden können.

Die Regelung wäre mit dem geltenden Recht besser abzustimmen. Nach dem Wortlaut der Regelung ist es nicht möglich, dass der Datenschutzbeauftragte als „Verantwortlicher nach § 9 VStG" bestellt werden kann und somit gegen ihn persönlich die Verhängung von Geldbußen möglich wäre. Das deswegen, weil die-

Wien 3 · Kundmanngasse 21
1031 Wien · Postfach 600
www.hauptverband.at
DVR 0024279

Hauptverband der
österreichischen
Sozialversicherungsträger

ser Beauftragte nicht die Aktionsmöglichkeiten hat, welche ihn verantwortlich machen könnten (vgl. § 9 Abs. 4 VStG „... der für den ihrer Verantwortung unterliegenden klar abzugrenzenden Bereich *eine entsprechende Anordnungsbefugnis zugewiesen ist* ..."). § 19 Abs. 3 des Entwurfes scheint aber davon auszugehen, dass dies der Fall sein könnte.

Aus den Art. 37 ff. der DSGVO ist keine Haftung des Datenschutzbeauftragten abzuleiten. Ebenso sieht das die Artikel-29-Datenschutzgruppe der EU, nach welcher die persönliche Verantwortung – soweit diese intern angesiedelt ist – beim Compliance-Officer bzw. Controlling liegt, während der Datenschutzbeauftragte eine beratende Funktion hat. Er ist zwar weisungsfrei, hat aber keine Anweisungsbefugnisse bzw. faktische Durchsetzungsmöglichkeiten.

Eine Verantwortlichkeit im Sinne des § 9 VStG könnte nur dann an den Datenschutzbeauftragen übertragen werden, wenn dieser – arbeits- und organisationsrechtlich – mit sehr weitgehenden Befugnissen ausgestattet wird (z. B. einem geschäftsführenden Verwaltungskörper Weisungen geben könnte).

Das würde allerdings dem Organisationsrecht der Sozialversicherung (und wohl auch anderer Selbstverwaltungskörper) widersprechen, welches die Verantwortung den Vorständen (Verbandsvorstand) gibt, welche als Selbstverwaltungskörper weisungsfrei sind (vgl. Art. 120b Abs. 1 B-VG, § 434, § 441f ASVG).

Dieser Anweisungsumfang wird nur bei leitenden Organen gegeben sein. Folgt man diesen Ansichten, ist es unzulässig, die Haftung nach § 9 VStG auf den Datenschutzbeauftragten zu übertragen.

Da in der laufenden Diskussion auch andere Ansichten vertreten werden, wäre dies wäre in den Erläuterungen klarzustellen.

Zu § 19 Abs. 5 DSG

Ergänzend wäre zu normieren, dass auch sogenannte „Inhouse-Töchter" von Behörden und öffentlichen Stellen (im Sinne des Vergaberechts) als „öffentliche Stellen" anzusehen sind und gegen sie keine Geldbußen verhängt werden können. Es wäre unsachlich, einerseits (vergaberechtlich, vgl. § 10 BVergG 2017 idF dessen Entwurfes) zu verlangen, eine Tochtergesellschaft „wie eine eigene Dienststelle" behandeln zu müssen bzw. zu dürfen, aber andererseits dieser Tochter durch das Datenschutzrecht Haftungen zu überbürden, deren Einhaltung sie eben wegen der engen Bindung an die Muttergesellschaften (Behörden etc.) gar nicht nachkommen könnten.

Wien 3 · Kundmanngasse 21
1031 Wien · Postfach 600
www.hauptverband.at
DVR 0024279

Hauptverband der
österreichischen
Sozialversicherungsträger

Zu § 32 Abs. 3 zweiter Satz DSG

Die Speicherdauer für Bilddaten von 72 Stunden ist prinzipiell für die Praxis zu kurz (vgl. Anmerkungen zu § 50b DSG 2000 in Dohr/Pollirer/Weiß/Knyrim).

Zu § 76 Abs. 2

Das Datenverarbeitungsregister (DVR) wird nur mehr zu Archivzwecken bis Ende 2019 fortgeführt. Gemäß Erläuterungen bleiben Registrierungsakte nicht aufrecht, selbst dann nicht, wenn sie auf einer Vorabkontrolle beruhen.

Die Regelung sollte überdacht werden. Es sollte klargestellt werden, dass erfolgte Registrierungen – insbesondere Anwendungen, die einer Vorabkontrolle unterliegen – weiterhin Gültigkeit besitzen. Nach den derzeitigen Erläuterungen ist nicht klar, wie mit bereits gemeldeten (teilweise auch genehmigten) Datenanwendungen umzugehen ist: Nach dem vorliegenden Entwurf wäre davon auszugehen, dass bei Wegfall der Geltung der Vorabbewilligung jedenfalls keine neuerliche (oder erstmalige) Datenschutz-Folgenabschätzung mehr notwendig ist.

Zu § 76 Abs. 5 DSG

Die Bestimmung sieht vor, dass Verletzungen, die zum Zeitpunkt des Inkrafttretens dieses Bundesgesetzes noch nicht anhängig gemacht wurden, nach der neuen Rechtslage zu beurteilen sind. Gemäß Erläuterungen ist jedoch auf die für den Täter günstigere Bestimmung abzustellen.

Dieses Günstigkeitsgebot sollte unmittelbar im Gesetzestext normiert werden (vgl. bspw. § 1 Abs. 2 VStG).

Andernfalls würde die Regelung für alle Normanwender eine massive Unklarheit schaffen. Es könnten (höhere) Strafen verhängt werden, die zum Zeitpunkt der Datenschutzverletzung nach der geltenden Rechtslage nicht möglich waren. Dies ist nicht gerechtfertigt und widerspricht einem grundlegenden strafrechtlichen Gedanken (nulla poena sine lege scripta, praevia, certa et stricta – strafrechtliches Rückwirkungs- und Analogieverbot).

Die Regelung stellt eine rückwirkende belastende Rechtsvorschrift dar und steht unseres Erachtens im Widerspruch zu Art. 7 EMRK.

Zu § 77 Abs. 2 DSG

Anstelle *„§ 1, § 7 Abs. 3 und § 62 Abs. 3* ***DSG 2000***" müsste *„§ 1, § 7 Abs. 3 und § 62 Abs. 3* ***DSG***" angeführt werden.

Wien 3 · Kundmanngasse 21
1031 Wien · Postfach 600
www.hauptverband.at
DVR 0024279

Hauptverband der
österreichischen
Sozialversicherungsträger

Datenschutz-Folgenabschätzung – Ergänzungsvorschlag

Die künftig verpflichtende Folgenabschätzung lässt noch breiten Gestaltungsspielraum. Die diesbezüglich bestehende Öffnungsklausel sollte genützt werden. Es sollte eine Ausnahme bei Datenanwendungen auf Basis gesetzlicher Grundlagen geschaffen werden. Zudem wären klare Regelungen zu Umfang und Ausgestaltung der Folgenabschätzung erforderlich.

Außerdem wäre zu normieren, dass für Datenverarbeitungen, die auf Grund von gesetzlichen Bestimmungen erforderlich werden, eine Datenschutz-Folgenabschätzung schon im Zuge des Gesetzwerdungsprozesses (Begutachtungsverfahrens) vorzunehmen und in den Materialien darzustellen ist.

Zu Art. 28 Abs. 2 DSGVO – Ergänzungsvorschlag

Diese Bestimmung wäre besser mit den Gegebenheiten des Wirtschaftslebens abzugleichen und müsste das Vergaberecht besser berücksichtigen.

Gemäß Art. 28 Abs. 2 DSGVO muss ein Auftragsverarbeiter eine gesonderte schriftliche Genehmigung des Verantwortlichen vor Inanspruchnahme eines weiteren Auftragsverarbeiters einholen.

Die Umsetzung dieser Bestimmung gestaltet sich teilweise als unmöglich: Bietet beispielsweise ein Rechenzentrumsbetreiber (Auftragsverarbeiter) Dienstleistungen wie Cloud-Dienste, Applikation-Service-Providing oder auch nur die Servicierung von Apps an, welche Daten zentral am Server speichern, wird er eine Vielzahl von Verantwortlichen servicieren.

Für den Fall der Beauftragung eines neuen Wartungspartners für ein Speichersystem/Server etc. (z. B. Insolvenz/Konkurs des bisherigen Partners), welcher im Rahmen der Wartung Zugriff auf die von den Verantwortlichen gespeicherten Daten erhalten kann, dann müsste der Rechenzentrumsbetreiber zuvor von einer Vielzahl von Verantwortlichen eine entsprechende Genehmigung einholen.

Wenn nur einer der Verantwortlichen die Beauftragung ablehnt, darf der Wartungspartner nicht beauftragt werden. So kann es passieren, dass sämtliche potentielle Wartungspartner von verschiedenen Verantwortlichen abgelehnt werden und damit die Sicherheit der Datenverarbeitung gefährdet ist.

Das Problem verschärft sich, wenn der Auftragsverarbeiter dem Bundesvergabegesetz unterliegt und die (Wartungs-)Leistung ausschreiben muss. Nach Durchführung des Vergabeverfahrens ist grundsätzlich eine Auftragserteilung erforderlich, es sei denn, es liegt ein Widerrufsgrund vor. Die fehlende daten-

Wien 3 · Kundmanngasse 21
1031 Wien · Postfach 600
www.hauptverband.at
DVR 0024279

Hauptverband der
österreichischen
Sozialversicherungsträger

schutzrechtliche Zustimmung zur Beauftragung, stellt jedoch keinen Widerrufsgrund dar.

Es wäre daher erforderlich klarzustellen, wie mit dieser Fallkonstellation umzugehen ist.

Mit freundlichen Grüßen
Für den Hauptverband:

Dr. Josef Probst
Generaldirektor

Wien 3 · Kundmanngasse 21
1031 Wien · Postfach 600
www.hauptverband.at
DVR 0024279