DORDA

Bundeskanzleramt
Ballhausplatz 2
1010 Wien

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

Wien, 22.6.2017

Betrifft: Stellungnahme zum Entwurf des Datenschutz-Anpassungsgesetzes 2018

Sehr geehrte Damen und Herren!

Wir nehmen als Praktiker mit jahrelanger Erfahrung mit dem alten Datenschutzregime, aber auch bereits mit Umsetzungsprojekten unter der DSGVO, und ausgewiesene Experten im IT Bereich wie folgt zum Entwurf des Datenschutz-Anpassungsgesetzes 2018 und den damit in Aussicht gestellten Änderungen des Datenschutzgesetzes ("DSG Neu") Stellung:

A. ALLGEMEINE EINSCHÄTZUNG

Das DSG Neu ist in seiner Gesamtheit ein gelungener, gut lesbarer Entwurf. Insbesondere begrüßen wir den zurückhaltenden Ansatz, womit nur die unbedingt erforderlichen Regelungen der DSGVO umgesetzt und Öffnungsklauseln bewusst vorsichtig genutzt werden. Diese Minimalumsetzung dient der Vollharmonisierung des europäischen Datenschutzrechts und führt zu wesentlichen Erleichterungen im grenzüberschreitenden Wirtschaftsleben. Im Gegenteil würde eine exzessive Ausnutzung der Regelungsspielräume und etwaige daraus resultierende Sonderbestimmungen für in Österreich tätige Unternehmen zu Nachteilen der österreichischen Wirtschaft im grenzüberschreitenden Verkehr und damit für den Wettbewerbsstandort Österreich führen.

In diesem Lichte ist der in den Erläuterungen (Allgemeiner Teil, Seite 1 ff) mehrfach betonte Vorbehalt, dass weitere Abweichungen von der DSGVO bzw dem DSG Neu in spezifischen Materiengesetzen folgen können, kritisch: Eine Regelung datenschutzrechtlicher Bestimmungen in Sondergesetzen würde nicht nur zu den oben dargelegten Wettbewerbsnachteilen, sondern on top auch zu einer in der Praxis schlecht handhabbaren Zersplitterung und damit Rechtsunsicherheit führen. Dementsprechend regen wir an, dass der Gesetzgeber auch in Zukunft hinsichtlich möglicher Öffnungsregelungen zurückhaltend Gebrauch macht. Auch aus dem gleich erläuternden zeitlichen Aspekt wäre ein verspätetes Nachschieben weiterer österreichischer

Sonderbestimmungen fatal: Die Unternehmen befassen sich bereits jetzt mit der Umsetzung des komplett neuen Datenschutzregimes und würden spätere Sonderregelungen bereits getätigte Aufwände frustrieren.

Um den österreichischen Unternehmen die notwendige Vorbereitungszeit für die erforderliche Umstellung ihrer Datenverarbeitungen und Prozesse an das neue, strengere Regime zu gewähren, ist ein Erlass des DSG Neu noch in der laufenden Legislaturperiode unbedingt erforderlich. Der kürzlich bereits erfolgte Erlass des Ministerialentwurfs als Regierungsvorlage trotz laufendem Stellungsnahmenprozess lässt die Intention des Gesetzgebers an einer zeitnahen Verabschiedung der neuen Regelungen erkennen. Es bleibt zu hoffen, dass der politische Schulterschluss für die tatsächliche Beschlussfassung im Sinne der Notwendigkeit für die österreichische Wirtschaft geschafft wird. Allerdings sollten trotz der Zeitknappheit die während der Begutachtungsfrist eingelangten, begründeten Stellungnahmen jedenfalls sorgfältig berücksichtigt werden. So ist dem Gesetzesentwurf wie einleitend angemerkt eine hohe Qualität zu attestieren. Dennoch gibt es aus Praktikersicht aber dennoch einige wesentliche Themen, die im Sinne des Schutzes des Wirtschaftsstandortes und zur Schaffung der Rechtssicherheit zu berücksichtigen wären. Der im Folgenden artikulierte Klarstellungsbedarf ist insbesondere auch vor dem mit der DSGVO geänderten Zugang zur Datenschutz-Compliance zu sehen: Einerseits hat sich die Prüfung der Einhaltung der datenschutzrechtlichen Vorgaben weg von der Behörde hin zum Unternehmen verlagert. Jeder Unternehmer muss nun für sich selbst ex ante ohne Behördenverfahren prüfen, ob und wie es Daten verarbeiten darf, hat die Vorgänge ordnungsgemäß zu dokumentieren und gegebenenfalls Folgenabschätzungen zu treffen. Die Behörde prüft die Einhaltung der Datenschutzregelungen erst ex-post. Bei Verstößen drohen drastische Geldstrafen. In diesem Lichte ist es wichtig, den Unternehmen möglichst klare Anleitungen und Erläuterungen an die Hand zu geben, um eine Einhaltung der sehr komplexen Bestimmungen zu ermöglichen und aus bloßem Unwissen resultierende Verstöße zu vermeiden.

Aufgrund der beabsichtigten Harmonisierung beschränkt sich diese Stellungnahme auf die tatsächlichen (unionsrechtskonformen) Möglichkeiten des österreichischen Gesetzgebers nach der DSGVO. In diesem Zusammenhang regen wir wie folgt an:

B. ANMERKUNGEN / KRITIKPUNKTE

1. Trennung des Dritten Hauptstücks vom DSG Neu

Grundsätzlich ist das DSG Neu übersichtlich strukturiert. Allerdings regen wir an, das dritte Hauptstück ("*Verarbeitung personenbezogener Daten für Zwecke der Sicherheitspolizei, des polizeilichen Staatsschutzes, des militärischen Eigenschutzes, der Aufklärung und Verfolgung von Straftaten, der Strafvollstreckung und des Maßnahmenvollzugs*") von den allgemeinen datenschutzrechtlichen Bestimmungen zu trennen und entweder (i) an das Ende des DSG Neu oder besser (ii) in ein eigenes Gesetz zu verschieben. Gerade unerfahrene Leser werden von den ähnlich lautenden

DORDA

Bestimmungen des im Gesetz eingebetteten dritten Hauptstücks und deren Anwendungsbereich irritiert und fehlgeleitet sein.

2. § 3 DSG Neu als Ausführung einer inhärenten Schranke der DSGVO

Die Bestimmung des § 3 DSG Neu, wonach eine Einschränkung der Verarbeitung ausreichend ist, solange die Berichtigung oder Löschung aus wirtschaftlichen oder technischen Gründen nicht unverzüglich möglich ist, ist als pragmatisch und praxisnah zu begrüßen. Tatsächlich stoßen auch modernste IT-Systeme bei der Anforderung, einzelne Datensätze sofort und aus sämtlichen Kopien (wie insbesondere Backups) zu entfernen, an ihre Grenzen. Diesen wesentlichen Umstand hat der europäische Gesetzgeber bei der Formulierung der Art 16 und Art 17 Abs 1 DSGVO allerdings nicht ausreichend klar berücksichtigt. Lediglich Erwägungsgrund 39 sieht vor, dass "*alle vertretbaren Schritte unternommen werden*" müssen, "*damit unrichtige personenbezogene Daten gelöscht oder berichtigt werden*". Auf dieser Basis ist mit guten Gründen argumentierbar, dass die DSGVO beim Abstellen auf eine "*unverzügliche*" Löschung oder Berichtigung tatsächlich als inhärente Schranke "*sobald technisch/wirtschaftlich möglich*" meint.

Um den möglichen Einwand einer Unionswidrigkeit hintanzuhalten und die praxisnahe Regelung langfristig zu festigen, empfehlen wir daher die Aufnahme eines entsprechenden Hinweises auf den Erwägungsgrund 39 in den Erläuternden Bemerkungen zum DSG Neu.

3. Bisher erteilte Einwilligungserklärungen weiterhin gültig

In der Praxis basiert eine Vielzahl an Datenverarbeitungen auf Zustimmungserklärungen der Betroffenen. Diese entsprechen den strengen Voraussetzungen des DSG 2000, das in Österreich ein über die bisher geltende Datenschutzrichtlinie 95/46/EG hinausgehendes Datenschutzniveau sicherstellt. Zur Steigerung der Rechtssicherheit in der Praxis – sowohl aus Unternehmer- als auch Betroffenensicht – ist daher (zumindest in den Erläuternden Bemerkungen) im DSG Neu eine Klarstellung erforderlich, dass rechtswirksam erteilte Einwilligungen weiterhin gültig bleiben. In Deutschland ist eine entsprechende Klarstellung im September 2016 durch einen Beschluss des Düsseldorfer Kreises (ein Gremium bestehend aus Vertretern aller deutschen Datenschutzbehörden) erfolgt (abrufbar unter https://www.lda.bayern.de/media/dk_einwilligung.pdf). Eine parallele Regelung auch im DSG Neu ist aus Praxissicht absolut wünschenswert.

4. Altersgrenze für die Einwilligung eines Kindes auf 14 Jahre senken

Die DSGVO sieht in Art 8 Abs 1 DSGVO die Möglichkeit vor, das Mindestalter für eine gültige Einwilligung eines Kindes von derzeit 16 Jahren auf bis zu 13 Jahre zu senken. Wir regen in diesem Zusammenhang an, diese Öffnungsklausel zu nützen und die Altersgrenze mit 14 Jahren festzusetzen. Das entspricht der in § 21 ABGB seit jeher etablierten österreichischen Abgrenzung zwischen unmündigen und mündigen Minderjährigen: So ist dieser Bestimmung folgend in der Praxis davon auszugehen, dass

Kinder im Alter von 14 Jahren bereits über ausreichende Einsichts- und Urteilsfähigkeit verfügen. Gleiches muss daher auch im Hinblick auf Dienste der Informationsgesellschaft gelten und somit für die informierte Einwilligung iSd DSGVO. Vielmehr besteht gerade hinsichtlich der Nutzung von Websites, Onlinediensten und Apps eine besondere Affinität von Kindern dieser Altersklasse. Im Onlinebereich 14 und 15 Jährige von der Geschäftsfähigkeit auszunehmen erscheint dagegen nahezu praxisfern und würde de facto auch zu großen Problemen führen: Es ist davon auszugehen, dass dennoch zahlreiche Minderjährige die gerade an sie gerichteten Onlineservices unter Akzeptanz der Datenschutzbestimmung nutzen würden. Mangels effektiver Überprüfungsmöglichkeiten des tatsächlichen Alters der User bliebe das in der Regel bis zum einem konkreten Eskalationsfall unentdeckt. Es käme damit zu einem unnötigen und sachlich nicht gerechtfertigten Auseinanderfallen der Praxis und Rechtslage, die zu entsprechenden Rechtsproblemen führen würde.

5. Datenschutz-Folgenabschätzung für gesetzlich erforderliche Verarbeitungen nicht erforderlich

Art 35 Abs 10 DSGVO sieht die Möglichkeit vor, dass ein Mitgliedsstaat erklärt, dass gesetzlich erforderliche Datenverarbeitungen keine Datenschutz-Folgenabschätzung benötigen. Dies ist stringent, da bei derartigen Verarbeitungen bereits der Gesetzgeber mit dem Erlass der jeweiligen Rechtsgrundlage eine positive, die Verarbeitung erlaubende Abwägung getroffen hat. Andernfalls müsste man dem Gesetzgeber unterstellen, dass derartige Verarbeitungspflichten ohne vorherige Interessensabwägung in das gesetzliche Vorgaben gefunden haben. Darüber hinaus ist es auch in der Praxis nicht sinnvoll, dass sämtliche Unternehmen eine inhaltsgleiche Folgenabschätzung über zwingend erforderliche Datenverarbeitungen vornehmen.

Daher regen wir an, im DSG Neu eine Bestimmung aufzunehmen, wonach für gesetzlich geregelte Datenverarbeitungen keine Datenschutz-Folgenabschätzung erforderlich ist.

6. Datenschutz-Folgenabschätzung für genehmigte Verarbeitungen nicht erforderlich

Darüber hinaus ist auch bei bereits von der Datenschutzbehörde (zB im Rahmen der Vorabkontrolle) genehmigten Verarbeitungen eine Datenschutz-Folgenabschätzung nicht erforderlich: Aufgrund der vorgelagerten, detaillierten und im europäischen Vergleich strengen Einzelfallprüfung durch die Datenschutzbehörde ist grundsätzlich auszuschließen, dass solche Verarbeitungen ein "*voraussichtlich hohes Risiko*" für die Betroffenen mit sich bringen können (siehe Art 35 Abs 1 DSGVO) – sonst hätte die Behörde die Genehmigung auch bereits nach dem noch geltenden DSG 2000 verweigern müssen. Dementsprechend wäre eine zusätzliche Folgenabschätzung beim Verarbeiter mit Anwendbarkeit der DSGVO eine unnötige Zweigleisigkeit. Wir regen daher eine Klarstellung (zumindest in den Erläuternden Bemerkungen) im DSG Neu an, dass bei bereits behördlich genehmigten Verarbeitungen keine Datenschutz-Folgeabschätzung erforderlich ist.

DORDA

7. Datenschutzbeauftragter kann nicht verantwortlicher Beauftragter iSd § 9 VStG sein

Im DSG Neu fehlt aus unserer Sicht eine Klarstellung, dass der nach Art 37 DSGVO zu bestellende Datenschutzbeauftragte nicht (gleichzeitig) verantwortlicher Beauftragter gemäß § 9 Abs 2 VStG sein kann. Eine solche Doppelbenennung würde in der Praxis nämlich unweigerlich zu einem nach Art 38 Abs 6 DSGVO unzulässigen Interessenkonflikt führen: Während der Datenschutzbeauftragte im wesentlichen Beratungs- und Überwachungsfunktionen ausübt (siehe Art 39 DSGVO), muss der verantwortliche Beauftragte auch eine entsprechende Anordnungsbefugnis haben (siehe § 9 Abs 4 VStG). Durch die Vereinigung beider Funktionen in ein und derselben Person entsteht eine unzulässige – und wohl auch sinnwidrige – Selbstkontrolle (der Datenschutzbeauftragte kontrolliert sich selbst). Das steht im klaren Widerspruch zu den Vorgaben der DSGVO.

8. Bestimmungen zur Datenverarbeitung zu Zwecken der Forschung und Statistik nicht mehr systemkonform

Die DSGVO lässt durchgängig eine praxisnahe Privilegierung von Datenverarbeitungen zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken erkennen. Dementsprechend enthält sie auch eine Reihe an Öffnungsklauseln für den nationalen Gesetzgeber. Diese Regelungsspielräume wurden im Entwurf des DSG Neu (konkret dessen § 25) allerdings kaum berücksichtigt. Vielmehr wurden überwiegend die bisherigen, strengeren Sonderbestimmungen des DSG 2000 übernommen. Das führt im Ergebnis zu einer (so wahrscheinlich nicht gewollten und unionsrechtlich kritischen) Verschärfung des Datenschutzniveaus im europäischen Vergleich und damit zu Nachteilen für den Wettbewerbsstandort Österreich sowie den medizinischen Fortschritt:

Gemäß § 25 Abs 2 Z 2 DSG Neu sind Datenverarbeitungen für Zwecke wissenschaftlicher Forschung unter anderem auf Basis einer Einwilligung der betroffenen Person zulässig. Diese Formulierung legt nahe, dass der österreichische Gesetzgeber auf die allgemeinen (strengen) Voraussetzungen der Art 7 und Art 6 Abs 1 lit a DSGVO abstellt. Konkret sieht die DSGVO in ErwG 33 aber vor, dass die betroffene Person ihre "*Einwilligung für bestimmte Bereiche wissenschaftlicher Forschung*" abgeben kann, "*wenn dies unter Einhaltung der anerkannten ethischen Standards der wissenschaftlichen Forschung geschieht*". Es ist damit schon nach dem Wortlaut keine Zustimmung zu einem im Vorhinein konkreten Zweck erforderlich. Dabei wird praxisnah berücksichtigt, dass gerade in diesem Bereich die konkreten Forschungszwecke meist noch nicht im Zeitpunkt der Erhebung der Daten vollständig angegeben werden können. Das DSG Neu steht in der derzeitigen Formulierung scheinbar im offenen Widerspruch zu der in der DSGVO vorgesehenen Lockerung des Zweckbindungsgrundsatzes. Damit ist die österreichische Umsetzung – wohl ungewollt – unionsrechtswidrig. Der in der DSGVO verankerte Grundsatz der erleichterten, da offeneren Zustimmung im Bereich wissenschaftlicher Forschung ist für die Praxis zudem tatsächlich von enormer Bedeutung und sollte auch ausdrücklich im DSG Neu vorgesehen werden. Hierzu sollte entweder im Gesetzestext

eine Klarstellung, dass hier die Kriterien der Zustimmung herabgesetzt sind, oder aber zumindest in den Erläuternden Bemerkungen ein entsprechender Verweis auf die DSGVO und die Erwägungsgründe erfolgen.

Weiters entspricht die in § 25 Abs 2 Z 3 DSG Neu vorgesehene Genehmigung der Datenschutzbehörde für Datenverarbeitungen zu Forschungs- und Statistikzwecken nicht dem System der DSGVO: In Abkehr von der bisherigen Rechtslage sieht das neue Regime nämlich vor, dass jeder Verantwortliche selbstverantwortlich zu prüfen hat, ob eine Datenverarbeitung im Einzelfall zulässig ist (vgl die Bestimmungen zum Verzeichnis von Verarbeitungstätigkeiten und der Datenschutz-Folgenabschätzung in Art 33 und Art 35 DSGVO). Erst *ex post* im Anlassfall (also nicht wie bisher nach dem DSG 2000 *ex ante*) prüft die Datenschutzbehörde, ob eine Verarbeitung rechtmäßig ist. Zudem würden zeitraubende Genehmigungsverfahren gerade in diesem hochspezialisierten Bereich den Wettbewerbsstandort Österreich erheblich unattraktiver machen. Darüber hinaus spießt sich die Pflicht zur Vorabgenehmigung durch die Datenschutzbehörde nach § 25 DSG Neu mit der selbstverantwortlich vorzunehmenden Datenschutz-Folgenabschätzung nach Art 35 DSGVO: De facto ist es sinnwidrig, dass der Verantwortliche für eine schon genehmigte Datenverarbeitung noch zusätzlich eine eigenständige Risikofolgenabschätzung durchführen soll.

Im Ergebnis führt die Genehmigungspflicht daher zu einer nicht mehr systemkonformen Überbürokratisierung der Datenverarbeitungen zu Forschungszwecken sowie zu einer Benachteiligung der Forschung im internationalen Vergleich. Wir regen daher an, die Genehmigungspflicht im DSG Neu (konkret daher die §§ 25 Abs 2 Z 3 sowie Abs 3 und Abs 4) zu streichen. Stattdessen schlagen wir vor, dass die Verarbeitung besonderer Kategorien von Daten zu Forschungszwecken (in Anlehnung an die deutsche Bestimmung des § 27 Abs 1 BDSG idF DSAnpUG-EU) auf Grundlage überwiegend berechtigter (öffentlicher) Interessen zulässig ist, sofern auch ein positives Votum einer Ethikkommission vorliegt. Alternativ kann die Genehmigungspflicht an eine kurze Frist für die Bearbeitung durch die Datenschutzbehörde (etwa zwei Monate) geknüpft (vergleiche die bisherige Vorabkontrolle) werden. Dies in Verbindung mit der Regelung, dass keine Folgenabschätzung durchzuführen ist (vgl die Öffnungsklausel in Art 35 Abs 10 DSGVO).

9. System der Verhängung von Geldbußen verfassungsrechtlich bedenklich

Im Sinne der Art 82 ff DSGVO ist (nicht nur "*kann*", wie im Entwurf) das Unternehmen statt einer natürlichen Person zu bestrafen. Die in § 19 DSG Neu erfolgte Umsetzung ist jedoch vor dem Hintergrund der enorm hohen Strafdrohungen der DSGVO verfassungsrechtlich bedenklich und regen wir daher an, dass (i) die Verhängung von Geldbußen in die Zuständigkeit eines unabhängigen Gerichts (entweder die ordentlichen Gerichte oder das Bundesverwaltungsgericht) gelegt wird (allenfalls mit Anzeigemöglichkeit der Datenschutzbehörde und Stellungnahme des Verantwortlichen), (ii) natürliche Personen bei besonderen Umständen lediglich eine geringere Strafe erhalten können und (iii) ein ausdrücklicher Ausschluss des Rückgriffs auf natürliche Personen gleichlautend zu § 11 Verbandsverantwortlichkeitsgesetz aufgenommen wird.

DORDA

Die verfassungsrechtlichen Bedenken ergeben sich nicht zuletzt aus den zu § 99d BWG – der nach den Erläuternden Bemerkungen als Vorlage zu § 19 DSG Neu dient – bereits beim Verfassungsgerichtshof beantragten verfassungsrechtlichen Überprüfung durch das Bundesverwaltungsgericht (vgl BVwG 21.11.2016, W2302138107-1; BVwG 24.11.2016, W210 2138108-1; 23.12.2016, W1072118633-2; BVWG 22.12.2016 W148, 2118633-1): Konkret sei die nahezu idente Bestimmung des BWG insbesondere nicht mit Art 91 B-VG vereinbar, da es sich um eine strafrechtliche Sanktion handle und die Verhängung derart hoher Strafen die Zuständigkeit der ordentlichen Gerichte begründe. Außerdem verstoße dieses System gegen das Verbot der Doppelbestrafung (Art 4 EMRK), da neben der juristischen Person auch die nach § 9 Verwaltungsstrafgesetz bestellte natürliche Person haften kann. Der idente Ansatz wurde nun im DSG Neu verankert, wobei nach der DSGVO sogar noch höhere (!) Strafen drohen.

Zusätzlich unterscheidet das DSG Neu nicht nach der Rechtsform der von einer etwaigen Geldbuße betroffenen juristischen Person: So gibt es insbesondere bei Einzelunternehmern und Personengesellschaften aus haftungsrechtlicher Sicht keine juristische Person, die vorrangig zur Haftung herangezogen werden könnte. Im Gegenteil hat bei diesen Rechtsformen immer die dahinterstehende natürliche Person uneingeschränkt für etwaige Geldbußen einzustehen. Dies kann bei der von der DSGVO geforderten Strafhöhe in der Praxis nicht durchschlagen.

* * * * *

Für Rückfragen stehen wir jederzeit gerne zur Verfügung.

Mit freundlichen Grüßen

DORDA Datenschutzteam

Dr Axel Anderl, LLM
Partner
+43 1 533 47 95 – 23
axel.anderl@dorda.at

MMag Dr Felix Hörlsberger
Partner
+43 1 533 47 95 – 17
felix.hoerlsberger@dorda.at

Mag Nino Tlapak, LLM
Rechtsanwaltsanwärter
+43 1 533 47 95 – 23
nino.tlapak@dorda.at

Mag Dominik Schelling
Rechtsanwaltsanwärter
+43 1 533 47 95 – 23
dominik.schelling@dorda.at