Überblick über den Entwurf

des neuen

österreichischen DSG

Ab 25.5.2018 wird die Datenschutzgrundverordnung („DSGVO“) die neue, harte Realität im Datenschutzrecht sein. Der nationale Gesetzgeber ist berechtigt, einzelne Punkte der DSGVO in der Form eines nationalen Begleitgesetzes zu konkretisieren. Der lang ersehnte Entwurf zu diesem österreichischen Begleitgesetz wurde am 12.5.2017 als **Datenschutz-Anpassungsgesetz 2018 („DSG“)** verlautbart. Wir haben für Sie die **wichtigsten Punkte des DSG zusammengefasst**.

Bei Rückfragen wenden Sie sich bitte an:

Dr. Rainer Knyrim, Rechtsanwalt und Partner bei Knyrim Trieb Rechtsanwälte OG, E-Mail: ky@kt.at, T: +43 1 909 30 70

Dr. Gerald Trieb, LL.M., Rechtsanwalt und Partner bei Knyrim Trieb Rechtsanwälte OG, E-Mail: gt@kt.at, T: +43 1 909 30 70

Dr. Tobias Tretzmüller, B.A., Rechtsanwaltsanwärter bei Knyrim Trieb Rechtsanwälte OG, E-Mail: tt@kt.at, T: +43 1 909 30 70

Inhaltsverzeichnis:

§ 1 DSG – Grundrecht auf Datenschutz

Diese Bestimmung normiert wie bisher im Verfassungsrang, dass **jede natürliche Person Anspruch auf Geheimhaltung** der **sie betreffenden personenbezogenen Daten hat**.

Dieses Grundrecht gilt auch im Verhältnis Privater zueinander[1]. Aus der früheren Formulierung des bisherigen § 1 DSG 2000 weggefallen ist die „Achtung des Privat- und Familienlebens."

Anders als das DSG 2000 werden die DSGVO und das DSG die **Daten juristischer Personen nicht (mehr) schützen**. Etwaige dadurch bestehende Rechtslücken, insbesondere betreffend Geschäfts- und Betriebsgeheimnissen, sollen durch die korrespondierende Geheimnisschutz-RL (EU) 2016/943[2] abgedeckt werden.

§ 1 Abs 2 DSG regelt wie bisher, unter welchen Voraussetzungen **Beschränkungen des Grundrechts** zulässig sind, wobei ein neuer Satz eingefügt wurde, laut dem die Beschränkungen notwendig und verhältnismäßig und, insbesondere im Hinblick auf den Zweck, die verarbeiteten Daten und die Art der Verarbeitung, für die betroffenen Personen vorhersehbar sein muss. Dieser neue Satz wird, da er eine sehr enge Verwendungsmöglichkeit der Daten implizieren zu scheint, im Lichte des Art 6 Abs 4 DSGVO zu lesen sein, der eine – im Entstehungsprozess sehr umstrittene – Aufweichung des Zweckbindungsprinzips zB für Big Data Anwendungen zulässt. Die direkt anwendbare DSGVO geht nämlich auch nationalem Verfassungsrecht[3] vor, dass daher im Sinn der DSGVO angewandt werden muss.

§ 2 DSG – Anwendungsbereich

Das DSG gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten, sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind.

---

[1] Im Übrigen das einzige Grundrecht, welches in dieser Deutlichkeit eine unmittelbare Drittwirkung entfaltet.

[2] Richtlinie (EU) 2016/943 des Europäischen Parlaments und des Rates vom 08.06.2016 über den Schutz vertraulichen Know-Hows und vertraulicher Gechäftsinformationen vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung.

[3] Ausgenommen den Grundprinzipien der Verfassung.

Somit werden künftig auch weiterhin nicht nur elektronisch verarbeiteter Daten, sondern **auch nichtautomatisiert verarbeiteter Daten** dem Datenschutzrecht unterliegen. Das bedeutet, dass auch Papierunterlagen dem Datenschutzrecht unterliegen können, sofern diese in Form eines Dateisystems (zB einer Kartei) strukturiert gesammelt sind.

§ 3 DSG – Durchführungsbestimmung zu Backups

Kann die Berichtigung oder Löschung von automationsunterstützt verarbeiteten personenbezogenen Daten nicht unverzüglich erfolgen, weil diese aus wirtschaftlichen oder technischen Gründen nur zu bestimmten Zeitpunkten vorgenommen werden kann, so ist die Verarbeitung der betreffenden personenbezogenen Daten mit Wirkung nach Art 18 Abs 2 DSGVO bis zu diesem Zeitpunkt einzuschränken.

Diese Bestimmung entspricht der schon bisher bestehende österreichische Regelung und tut der Praxis Genüge, wonach Daten, die in **Backups** gespeichert wurden und aus technischen Gründen nicht sofort gelöscht werden können, aus den Backups „herauswachsen“ dürfen. Neu ist aber die Verpflichtung, diese Daten bis zur Löschung für die Verarbeitung zu sperren.

§ 4 und 5 DSG – Datenschutzbeauftragter, insbes. im öffentlichen Bereich

Wie erwartet erhält der Entwurf keine über die DSGVO hinausgehende Verpflichtung, einen Datenschutzbeauftragten zu bestellen, da zu vermuten ist, dass die Wirtschaftskammer wie schon bisher vehement dagegen wäre, dass weitere Belastungen für Unternehmen geschaffen werden. § 4 des Entwurfes enthält allerdings eine **Verschwiegenheitsverpflichtung** und ein **Aussageverweigerungsrecht** für Datenschutzbeauftragte.

In Konkretisierung der Art 37 ff DSGVO regelt § 5 des Entwurfes des DSG, dass **jedes Bundesministerium** einen oder mehrere **Datenschutzbeauftragte zu benennen hat**. Diese Datenschutzbeauftragen müssen interne Mitarbeiter sein und dürfen daher nicht extern hinzugezogen werden. Verfassungsrechtlich geregelt (Grundsatz der Gewaltenteilung) ist, dass auch die obersten Organe der Vollziehung der Kontrolle der Datenschutzbehörde unterliegen werden. Gegen Behörden und öffentliche Stellen können aber keine Geldbußen verhängt werden. Schadenersatzansprüche bleiben der betroffenen Person aber auch gegen öffentliche Stellen nicht unbenommen.

§ 6 DSG – Datengeheimnis

Diese Bestimmung verpflichtet den Arbeitgeber – wie nach bisheriger Rechtlage auch – dazu, dass er selbst, sowie seine Dienstleister und Mitarbeiter personenbezogene Daten aus Datenverarbeitungen, die ihnen ausschließlich auf Grund ihrer berufsmäßigen Beschäftigung anvertraut wurden, **geheim zu halten**. Ausdrücklich wird normiert, dass der Arbeitgeber seine Mitarbeiter über die Folgen einer Verletzung des Datengeheimnisses zu belehren hat und dieser vertraglich zu vereinbaren hat, dass das Datengeheimnis auch nach Beendigung des Arbeitsverhältnisses einzuhalten ist.

§ 10 DSG – Aufgaben der Datenschutzbehörde

Die Datenschutzbehörde („DSB“) hat Listen nach Art 35 Abs 4 und 5 DSGVO im Wege einer Verordnung kundzumachen.

Damit wird der DSB der gesetzliche Auftrag erteilt, dass diese betreffend der **Datenschutz-Folgenabschätzung** sowohl eine „**weiße Liste**“ als auch eine „**schwarze Liste**“ zu erstellen hat. In die „weiße Liste“ werden jene Datenverarbeitungstätigkeiten aufgenommen werden, für die keine Datenschutz-Folgenabschätzung erforderlich ist. In die „schwarze Liste“ hingegen jene Datenverarbeitungstätigkeiten, für die eine Datenschutz-Folgenabschätzung jedenfalls erforderlich ist.

Die Datenschutzbehörde soll überdies die einzige nationale Einrichtung werden, die die Befugnis hat, **nationale Datenschutz-Zertifizierungsstellen zu akkreditieren**.

§ 11 DSG – Befugnisse der DSB

§ 11 Abs 1 erster Satz DSG besagt, dass die Datenschutzbehörde „**im Falle eines begründeten Verdachtes auf Verletzung**“ der datenschutzrechtlichen Bestimmungen Überprüfungen durchführen kann. Das könnte im Umkehrschluss so verstanden werden, dass die Datenschutzbehörde nicht dazu ermächtigt ist, ohne konkreten Verdachtsmoment aktiv ermittelnd tätig zu werden. Art 58 Abs 1 lit b) DSGVO regelt allerdings, dass die DSB über „*sämtliche Untersuchungsbefugnisse verfügt, die es ihr gestatten…Untersuchungen in Form von Datenschutzüberprüfungen durchzuführen*.“

Die Datenschutzbehörde ist berechtigt, nach Verständigung des Inhabers, **Räume**, in welchen die Datenverarbeitung vorgenommen werden, **zu betreten**, **Datenverarbeitungsanlagen in Betrieb zu setzen**, die zu überprüfenden Verarbeitungen durchzuführen sowie **Kopien von Datenträgern herzustellen**.

Bei Gefahr in Verzug kann die Datenschutzbehörde die Weiterführung der Datenverarbeitung mit Bescheid unverzüglich untersagen (§ 11 Abs 4 DSG).

§ 11 Abs 5 DSG regelt, dass es der Datenschutzbehörde obliegt, im Rahmen ihrer Zuständigkeit **Geldbußen gegenüber natürlichen und juristischen Personen zu verhängen**[4].

§ 13 DSG – Beschwerde an die Datenschutzbehörde

Jede betroffene Person hat das Recht auf Beschwerde bei der Datenschutzbehörde, wenn sie der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen die DSGVO oder gegen das 1. oder 2. Hauptstück des DSG verstößt.

Die **Datenschutzbehörde kann bei sämtlichen Verstößen** gegen die sogenannten Betroffenenrechte, also beispielsweise gegen das Recht auf Auskunft, das Recht auf Löschung oder das Recht auf Datenübertragbarkeit, mittels Beschwerde **angerufen werden**. Für derartige Eingaben bei der Datenschutzbehörde werden **keine Verwaltungsabgaben** anfallen. Die Beschwerde muss aber bestimmten inhaltlichen Erfordernissen genügen.

Der Beschwerdeführer soll künftig innerhalb **von drei Monaten** ab Einbringung der Beschwerde über den Stand und das **Ergebnis der Ermittlungen unterrichtet werden**.

§ 17 DSG – Vertretung von betroffenen Personen

§ 17 DSG normiert, dass die betroffene Person das Recht hat, eine Einrichtung, Organisation oder Vereinigung ohne Gewinnerzielungsabsicht, die ordnungsgemäß gegründet ist und deren satzungsmäßige Ziele im öffentlichem Interesse liegen, zu beauftragen, in ihrem Namen eine Beschwerde bei der Datenschutzbehörde einzureichen und das Recht auf Schadenersatz in Anspruch zu nehmen.

Praktisch relevant wird somit sein, dass betroffene Personen durch den Entwurf die Möglichkeit bekommen sollen, **spezialisierte Organisationen** („**Datenschutz-NGOs**“) damit zu beauftragen, in ihrem Namen Beschwerde bei der Datenschutzbehörde zu erheben und sogar **Schadenersatzansprüche** bei Gericht einzuklagen. Von der durch Art 80 Abs 2 DSGVO eröffneten Option, dass diese Organisationen auch ohne konkrete Beauftragung der betroffenen Person einschreiten dürfen, macht der nati-

[4] Siehe dazu auch § 19.

onale Gesetzgeber im Entwurf keinen Gebrauch. Es bleibt abzuwarten, ob dieses Klagerecht auch endgültig in dieser Form umgesetzt wird.

§ 18 DSG – Haftung und Recht auf Schadenersatz

§ 18 DSG regelt, dass jede Person, der wegen eines Verstoßes gegen die DSGVO oder gegen das DSG ein materieller oder immaterieller Schaden entstanden ist, **Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter geltend machen kann**. Für Klagen auf Schadenersatz sind in erster Instanz die mit der Ausübung der Gerichtsbarkeit in bürgerlichen Rechtssachen betrauten **Landesgerichte** zuständig.

Klargestellt wird somit, dass – wie bisher – bei Klagen auf Schadenersatz wegen Datenschutzverletzungen die **Landesgerichte für Zivilrechtssachen** zuständig sein werden. Dabei hat der Kläger die Möglichkeit, die **Klage dort anhänglich zu machen, wo dieser seinen gewöhnlichen Aufenthalt oder Sitz hat**.

Aufgrund der Eigenzuständigkeit der Landesgerichte für Zivilrechtssachen besteht in diesen Verfahren eine **absolute Anwaltspflicht** (§ 27 Abs 1 ZPO).

§ 19 DSG – Verhängung von Geldbußen

Durch den Entwurf wird klargestellt, dass die **Datenschutzbehörde** jene Instanz sein **wird**, welche die **Geldbußen** von bis zu EUR 20 Mio oder 4% des weltweiten Konzernumsatzes **verhängen** wird.

Die Zielrichtung der Geldbußen ist im Entwurf dreigeteilt:

1. **Geldbuße gegen das Unternehmen wegen Verstoß durch Führungskraft**: Die **juristische Person selbst kann bestraft werden**, wenn der Verstoß gegen das Datenschutzrecht **durch eine Person** begangen wurde, die entweder allein oder als Teil eines Organs der juristischen Person gehandelt hat und eine **Führungsposition** innerhalb der juristischen Person innehat aufgrund (i) der Befugnis zur Vertretung der juristischen Person; (ii) der Befugnis, Entscheidungen im Namen der juristischen Person zu treffen, oder (iii) die eine Kontrollbefugnis innerhalb der juristischen Person innehat. Diese Geldbuße wird also dadurch ausgelöst, dass die **Führungs- oder Kontrollebene des Unternehmens selbst falsch handelt**.

2. **Geldbußen gegen das Unternehmen wegen Überwachungs- und Kontrollversagen:** Juristische Personen können wegen Verstößen gegen Bestimmungen der DSGVO laut dem Entwurf weiters verantwortlich gemacht werden, wenn die oben genannten Führungskräfte ihren

Aufsichtspflichten nicht nachgekommen sind und dadurch die Begehung eines Verstoßes durch eine für das Unternehmen tätige Person ermöglicht wurde ist. Wenn also aufgrund eines **fehlenden Datenschutz-Managementsystems** und einer fehlenden Implementierung eines **datenschutzrechtlichen Kontrollsystems** die DSGVO durch einen Mitarbeiter verletzt wird, **kann ebenfalls das Unternehmen selbst bestraft werden**.

3. **Geldbuße gegen verantwortlichen Beauftragten**: Weiters kann ein nach § 9 VStG bestellter verantwortlicher Beauftragter (zB eine für den Bereich Datenschutz verantwortlich gemachte Person) **persönlich bestraft werden**. Dies entspricht nicht der Zielrichtung der DSGVO, die nur das Unternehmen bestrafen will. Um diesen Konflikt abzuschwächen, kann die Datenschutzbehörde laut dem Entwurf **von einer Bestrafung** der natürlichen Person **absehen**, wenn gegen die juristische Person bereits eine Strafe verhängt wird und keine besonderen Umstände vorliegen, die einem Absehen von der Bestrafung entgegenstehen. Die Behörde kann somit von der Bestrafung insbesondere dann absehen, wenn dem Beauftragten kein persönlicher Vorwurf zu machen ist. Es ist aber zu erwarten, dass der Erste dennoch bestrafte Beauftragte den Instanzenzug beschreitet, um die DSGVO-Konformität dieser Regelung prüfen zu lassen.

Keine Strafen gegen Datenschutzbeauftragten: Der verantwortliche Beauftragte ist nicht zu verwechseln mit dem Datenschutzbeauftragten nach DSGVO, zu dem bereits die Guidelines der Art. 29-Gruppe zum Datenschutzbeauftragten klargestellt haben, dass dieser **nicht Ziel der Geldbußen der DSGVO ist**, wenn das Unternehmen einen DSGVO-Verstoß setzt. Auch der Entwurf des DSG spricht dem entsprechend keine Geldbußen des Datenschutzbeauftragten an.

Der Entwurf stellt auch klar, dass **gegen öffentliche Stellen keine Geldbußen verhängt** werden.

§ 20 ff DSG – Datenschutzrat

Beim Bundeskanzleramt ist wie bisher ein Datenschutzrat eingerichtet. Dieser nimmt zu Fragen von grundsätzlicher Bedeutung für den Datenschutz Stellung, fördert die einheitliche Fortentwicklung des Datenschutzes und berät die Bundesregierung in rechtspolitischer Hinsicht bei datenschutzrechtlich relevanten Vorhaben. Die Regeln – ua über die Zusammensetzung des Datenschutzrates – wurden im Vergleich zu bisher etwas adaptiert, der Datenschutzrat (der vor allem aus Vertretern der politischen Parteien besteht) benennt künftig selbst zwei Experten im Bereich des Datenschutzrechts.

§ 25 DSG – Verarbeitung zum Zweck der wissenschaftlichen Forschung und Statistik

Nach § 25 DSG darf der Verantwortliche für Zwecke wissenschaftlicher oder statistischer Untersuchungen, die keine personenbezogenen Ergebnisse zum Ziel haben, 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 pseudonymisiert personenbezogene Daten sind** und der Verantwortliche die Identität der betroffenen Person mit rechtlich zulässigen Mitteln nicht bestimmten kann.

Ansonsten dürfen für Datenverarbeitungen zum Zwecke wissenschaftlicher Forschung und Statistik, personenbezogene Daten nur verarbeitet werden

1. gemäß besonderen gesetzlichen Vorschriften,
2. mit Einwilligung der betroffenen Person oder
3. mit Genehmigung der Datenschutzbehörde.

Diese – praktisch vor allem in der Pharma- und Forschungsentwicklung sehr wichtige – Regelung wurde fast wortgleich der derzeitigen Gesetzeslage (§ 46 DSG 2000) entnommen. Dadurch kann **künftig auch weiterhin mit pseudonymisierten Daten – sogar von Dritten – geforscht und statistisch ausgewertet werden**, ohne dass die Einwilligung der betroffenen Personen erforderlich wäre!

§ 29 DSG – Verarbeitung personenbezogener Daten im Beschäftigungskontext

§ 29 DSG regelt, dass das **Arbeitsverfassungsgesetz („ArbVG“)** eine **Vorschrift im Sinne des Art 88 DSGVO ist**. Die dem Betriebsrat nach dem ArbVG zustehenden Befugnisse bleiben unberührt.

Die in Art 88 DSGVO enthaltene Öffnungsklausel bietet die Möglichkeit, im Bereich des Arbeitnehmerdatenschutzes neue Regelungen zu schaffen. Von dieser Möglichkeit will der österreichische Gesetzgeber aber offensichtlich keinen Gebrauch machen. Es wird somit die bisherige Rechtslage aufrechterhalten werden. Daher ist auch künftig bei der Einführung von Kontrollmaßnahmen und technischen Systemen zur Kontrolle der Arbeitnehmer, sofern diese Maßnahmen (Systeme) die Menschwürde berühren (so etwa regelmäßig bei Videoüberwachungen), eine **Betriebsvereinbarung**

zwischen Betriebsinhaber und Betriebsrat abzuschließen (§ 96 ArbVG). Bereits abgeschlossene Betriebsvereinbarungen sind weiterhin wirksam.

Unklar ist derzeit noch, ob durch die Benennung des ArbVG als Regelung iSd des Art 88 DSGVO in Österreich nun **direkt das Haftungsregime der DSGVO** (Geldbußen von bis zu EUR 20 Mio oder 4 % des Konzernumsatzes) **auf das ArbVG zur Anwendung kommt**. Art 83 Abs 5 lit d) DSGVO sieht nämlich vor, dass alle Pflichten, die von Mitgliedstaaten im Rahmen des Kapitel IX. (in diesem steht Art 88 DSGVO) erlassen wurden, mit den Geldbußen der DSGVO zu sanktionieren sind. Würde die Benennung des ArbVG – und vor allem die in Art 88 Abs 5 DSGVO geforderte Notifikation dieser Bestimmungen an die EU-Kommission – diesen Sanktionsmechanismus direkt auslösen, **würde dies bedeuten, dass allein der Nichtabschluss einer Betriebsvereinbarung künftig (mindestens) mit einem Strafrahmen von bis zu EUR 20 Mio sanktioniert wäre**! Sollten Betriebsvereinbarungen (bzw, sofern ein Betriebsrat nicht eingerichtet ist, Individualvereinbarungen nach § 10 Abs 1 AVRAG) bislang nicht abgeschlossen worden sein, **sollte dies vorsorglich bis längstens 25.05.2018 nachgeholt werden**.

§ 30 DSG – Bildverarbeitung

Eine praktisch wichtige Konkretisierung der DSGVO durch das DSG erfolgt hinsichtlich der Verarbeitung von Bildermaterial, wobei hier sowohl Fotos als auch Videos gemeint sind. Ist der Zweck der Bildverarbeitung, dass eine bestimmte Person abgelichtet werden soll, so ist **in den meisten Fällen deren Einwilligung zur Bildaufnahme einzuholen**. Dies gilt aber nicht, wenn das Foto oder Video nicht spezifisch auf eine Person ausgerichtet ist und es sich lediglich um ein privates Dokumentationsinteresse handelt (zB bei Urlaubsfotos). Sofern es sich nicht um private Aufnahmen handelt, bedarf es für eine Aufbewahrung für die Dauer von mehr als 72 Stunden einer Begründung. Im Falle einer Videoüberwachung kann die gefilmte Person auch vom Eigentümer oder Mieter der Liegenschaft, von dem aus die Überwachung ausgeht, Auskunft darüber verlangen, wer die Videoüberwachung aufgestellt hat.

§ 33 DSG – Kennzeichnung der Bildverarbeitung

Der Verantwortliche einer Bildaufnahme hat diese geeignet zu kennzeichnen.

Aus der Kennzeichnung hat jedenfalls der Verantwortliche eindeutig hervorzugehen, es sei denn, dieser ist den betroffenen Personen nach den Umständen des Falles bereits bekannt. Somit reicht auf den Hinweisschildern nicht ein bloßes Piktokramm, es ist auch der (Unternehmens-)Name des Verantwortlichen dort anzubringen.

Diese Kennzeichnungspflicht gilt jedoch nicht bei Bildaufnahmen, die ein privates Dokumentationsinteresse verfolgen ohne Intention eine bestimmte Person oder ein bestimmtes Objekt zu identifizieren.

§§ 34 bis 68 DSG – Verarbeitung personenbezogener Daten für Zwecke der Sicherheitspolizei, des polizeilichen Staatschutzes, des militärischen Eigenschutzes, der Aufklärung und Verfolgung von Straftaten, der Strafvollstreckung und des Maßnahmenvollzuges

Die Bestimmungen der §§ 34 bis 41 DSG sind die nationalen Umsetzungsbestimmungen zur Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl. Nr. L 119 vom 4.05.2016. Im Rahmen der Umsetzung wurde – soweit möglich – auf die zum Teil wortgleichen Regelungen in der DSGVO verwiesen.

§ 69 DSG – Verwaltungsstrafbestimmung

§ 69 DSG normiert für bestimmte Tatbestände, etwa der Verweigerung der Einschau durch die Datenschutzbehörde, dem vorsätzlichen widerrechtlichen Zugang zu einer Datenverarbeitung, vorsätzlichen Bruch des Datengeheimnisses oder der gesetzwidrigen Bildverarbeitung eine Geldstrafe von bis zu EUR 50.000,00. Diese Strafen sind subsidiär zur DSGVO und anderen Verwaltungsstrafbestimmungen. Es ist allerdings fraglich, ob dieses zusätzlichen Strafen neben der DSGVO zulässig sind, da die DSGVO diesbezüglich keine Öffnungsklausel enthält.

§ 70 DSG – Datenverarbeitung in Gewinn- oder Schädigungsabsicht

Wie auch bisher wird es künftig eine Strafdrohung von bis zu ein Jahr Freiheitsstrafe bei vorsätzlicher Datenverwendung in Gewinn- und Schädigungsabsicht geben, oder (neu) Geldstrafen bis zu 720 Tagessätzen (die sich nach dem Einkommen berechnen).

§ 76 DSG Übergangs- und Schlussbestimmungen

Datenverarbeitungsregister wird abgeschafft

Da die behördliche Meldepflicht mit der DSGVO durch die Pflicht zur Führung eines internen Verzeichnisses der Verarbeitungstätigkeiten („Verfahrensverzeichnis“) ersetzt wird, wird das von der Datenschutzbehörde geführte **Datenverarbeitungsregister abgeschafft**. Anhängige Registrierungsverfahren im DVR gelten mit 25.5.2018 als **eingestellt**. Das DVR ist von der Datenschutzbehörde allerdings laut dem Entwurf **bis zum 31.12.2019 zu Archivzwecken** fortzuführen, dh es kann dann zwar nicht mehr befüllt werden, bleibt bis dahin aber öffentlich abrufbar. Diese Abrufbarkeit, wie auch die Tatsache, dass die Informationen, die für das Verfahrensverzeichnis gesammelt werden müssen,

weitgehend ident mit jenen für die DVR-Meldungen sind, **machen Meldungen in das Datenverarbeitungsregister weiterhin sinnvoll** (abgesehen davon, dass die Meldeverpflichtung bis 24.5.2018 fortbesteht und jede Nichtmeldung bis zum 24.5.2017 eine Strafe bis EUR 10.000,-- auslösen kann).

Anhängige Verfahren

Am 25.05.2018 anhängige Verfahren betreffend der Überlassung und Übermittlung der Daten in Drittstaaten (nach § 13 DSG 2000), Wissenschaftlichen Forschung Statistik (nach § 46 DSG 2000) und Zurverfügungstellung von Adressen zur Benachrichtigung und Befragung von Betroffenen (nach § 47 DSG 2000) **werden fortgeführt**, **sofern die Genehmigung nach dem DSG oder der DSGVO erforderlich ist**.

Eine Genehmigung für die Übermittlung von Daten in Drittstaaten auf Basis künftiger **Standarddatenschutzklauseln** ist nach Art 46 DSGVO nicht mehr erforderlich sein, soferne nicht individuelle Klauseln nach Art 46 Abs 3 DSGVO genehmigt werden sollen. Art 46 Abs 5 DSGVO regelt, dass die bisher von der EU-Kommission erlassenen Standardvertragsklauseln weiter Geltung haben, solange die EU-Kommission diese nicht durch Neue ersetzt. Es ist daher zu vermuten, dass, wenn man die Überlassung und Übermittlung von Daten ins Ausland auf der Grundlage der aktuellen Standardvertragsklauseln genehmigen lassen will, ein solches Genehmigungsverfahren von der Datenschutzbehörde mit 25.5.2018 eingestellt werden wird, weil es dann nicht mehr erforderlich ist. Wer Rechtssicherheit bei internationalem Datenverkehr durch behördliche Genehmigung erlangen will (einmal erteilte Genehmigungen gelten auch unter der DSGVO weiter, solange sie nicht explizit wieder aufgehoben werden), sollte daher zur Sicherheit rechtzeitig (spätestens bis 24.11.2017) seinen Antrag einbringen, weil die Datenschutzbehörde grundsätzlich verpflichtet ist, binnen sechs Monaten zu entscheiden und damit die Entscheidung noch rechtzeitig vor dem 25.5.2018 ergehen könnte. Für eine Säumnisbeschwerde wäre aber auch dann keine Zeit mehr, sodass sich eine möglichst rasche Einbringung empfiehlt.

Der Entwurf regelt in § 76 Abs 8 weiters, dass datenschutzrechtliche Regelungen in anderen Materiegesetzen (zB Sicherheitspolizeigesetz) vom Entwurf unberührt bleiben, dh sie gelten weiter.

Sonstiges

Von einer Herabsetzung des **Kindesalters** im datenschutzrechtlichen Sinn auf unter sechzehn Jahre wird im Entwurf kein Gebrauch gemacht. Das bedeutet, dass die Verarbeitung von personenbezogenen Daten von Personen, die das sechzehnte Lebensjahr nicht vollendet haben, grundsätzlich nur dann rechtmäßig sein wird, sofern **eine gültige Einwilligung** in die Datenverarbeitung vorliegt. Diese

Regelung wird im Bereich der sozialen Medien relevant sein[5]. Denkbar ist, dass im Begutachtungsverfahren aber eine Herabsetzung auf 14 Jahre gefordert wird, um eine Anpassung an diese in Österreich übliche Altersgrenze („beschränkte Geschäftsfähigkeit“) zu erreichen.

Betreffend der – im Wortlaut der DSGVO unklaren – Verpflichtung zum Verzeichnis von Verarbeitungstätigkeiten (Art 30 DSGVO), der Datenschutz-Folgenabschätzung (Art 35 DSGVO) und der Kerntätigkeit iSd Art 37 Abs 1 DSGVO hinsichtlich der Verpflichtung zur Benennung eines Datenschutzbeauftragten enthält der Entwurf **keine Regelungen**, obwohl in diesen Bestimmungen Öffnungsklauseln enthalten sind.

Fazit

Im Unterschied zur DSGVO ist der Entwurf zum Datenschutz-Anpassungsgesetz 2018 klarer formuliert, wobei der praktischen Umsetzung vieler Verpflichtungen noch mit Spannung entgegengesehen werden muss.

Auffallend ist, dass der österreichische Gesetzgeber in der Konkretisierung einzelner Punkte der DSGVO weit weniger aktiv war als andere Mitgliedsstaaten. Die politische Vorgabe dürfte gewesen sein, nur die **Minimalerfordernisse** zu schaffen. Dennoch enthält der Entwurf auch einige sehr erfreuliche und sinnvolle Bestimmungen aus dem bisherigen Recht, etwa die Möglichkeit, zu löschende Daten aus Backups herauswachsen zu lassen, oder die Möglichkeit, weiter wissenschaftliche Forschung mit pseudonymisierten Daten betreiben zu können.

Eine **erhebliche Unsicherheit** bringt der **Verweis des Entwurfes auf das ArbVG** als österreichische Bestimmung zum Arbeitnehmer-Datenschutzrecht mit sich, denn wenn das ArbVG von Österreich als Arbeitnehmer-Datenschutzregelung bei der EU-Kommission notifiziert wird, dann steht eine **Sanktionierung des ArbVG** – zB bei Nichtabschluss einer Betriebsvereinbarung zur Arbeitnehmerdatenverarbeitung – **mit dem DSGVO-Strafrahmen von EUR 20 Mio oder 4% vom Umsatz im Raum**.

Aufgrund der anstehenden Neuwahlen am 15.10.2017 ist das Schicksal des Entwurfes ungewiss[6] und der zeitliche Werdegang des Entwurfes kann im Moment nicht abgeschätzt werden. Es ist aber auf-

[5] Siehe dazu ausführlich Dako 1/2017: Sensibilisierung ist der einzig wirksame Weg, *Knyrim/Schmidt/Souhrada-Kirchmayer*, Dako 2017/2 sowie ebenso in dieser Ausgabe: Datenschutz-Grundverordnung: Der neue Kinderschutz, *Pilgermair*, Dako 2017/4.

grund der Neuwahlen **kaum damit zu rechnen, dass der Entwurf noch 2017 fertig beschlossen sein wird.**

Unabhängig vom nun vorliegenden Entwurf und dessen Zukunft gilt es aber jedenfalls, sich weiterhin **mit Hochdruck auf den Stichtag 25.5.2018 vorzubereiten**, denn die DSGVO ist direkt anwendbar und formal bereits in Kraft, lediglich die Anwendung ist bis zu diesem Tag noch ausgesetzt.

Gerne stehen wir Ihnen bei Fragen zum **Datenschutz-Anpassungsgesetz 2018 oder bei der Vorbereitung auf die DSGVO** zur Verfügung.

Wien, am 25.5.2017

Zu den Autoren:

Dr. Rainer Knyrim ist Rechtsanwalt und Partner der Knyrim Trieb Rechtsanwälte OG, Wien. E-Mail: ky@kt.at

Dr. Tobias Tretzmüller, B.A. ist Rechtsanwaltsanwärter der Knyrim Trieb Rechtsanwälte OG, Wien. E-Mail: tt@kt.at

---

[6] Insbesondere aufgrund der im Entwurf enthaltenen Verfassungsbestimmungen und zu deren Beschlussfassung notwendigen 2/3-Mehrheit im Parlament.