Secur-Data Betriebsberatungsges.m.b.H.
1010 Wien, Fischerstiege 9
Tel. +43 (1) 533 42 07-0
Internet: www.secur-data.at E-Mail: office@secur-data.at

DSG-Info-Service

Mai 2017 Ausgabe Nr. 87

Sehr geehrter DSG-Paket-Kunde!
Sehr geehrter Leser!

Die EU-Datenschutz-Grundverordnung (EU-DSGVO) ist am 25. Mai 2016 in Kraft getreten und mit 25. Mai 2018 für alle EU-Mitgliedstaaten verpflichtend anzuwenden. Grundsätzlich ist eine EU-Verordnung unmittelbar anwendbar, die DSGVO enthält jedoch insgesamt 69 Öffnungsklauseln und Regelungsspielräume, die von den Mitgliedstaaten in einigen Fällen obligatorisch und in den meisten Fällen fakultativ genutzt werden können. Dadurch ist der nationale Gesetzgeber verpflichtet bzw. berechtigt, einzelne Punkte der DSGVO durch ein Begleitgesetz zu konkretisieren.

Am 12. Mai 2017 wurde der Entwurf zum bereits für Herbst 2016 versprochenen „Datenschutz-Anpassungsgesetz 2018“[1] verlautbart. Da die Begutachtungsfrist am 23. Juni 2017 endet und anschließend die entsprechenden Verhandlungen beginnen, ist mit großer Wahrscheinlichkeit nicht mehr mit dem Inkrafttreten dieses Gesetzes in der laufenden Legislaturperiode zu rechnen.

Der Entwurf des neuen Datenschutzgesetzes verfolgt das Ziel, nur die unbedingt erforderlichen Regelungen der DSGVO im innerstaatlichen Recht durchzuführen.

Gleichzeitig mit der DSGVO wurde auch die Richtlinie 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[2] *beschlossen. Diese Richtlinie muss in innerstaatliches Recht umgesetzt werden, was ebenfalls durch den gegenständlichen Entwurf (drittes Hauptstück des neuen Datenschutzgesetzes) erfolgen soll.*

Nachstehend werden die wichtigsten Punkte des DSG in Kurzform behandelt:

[1] https://www.parlament.gv.at/PAKT/VHG/XXV/ME/ME_00322/index.shtml

[2] http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32016L0680&qid=1496041890156

Datenschutz-Anpassungsgesetz 2018

Artikel 1
(Verfassungsbestimmung)

Änderung des Bundes-Verfassungsgesetzes

Das Bundes-Verfassungsgesetz – B-VG, BGBl. Nr. 1/1930, zuletzt geändert durch das Bundesverfassungsgesetz BGBl. I Nr. 62/2016, wird wie folgt geändert:

1. *[…]*

2. *[…]*

3. *Dem Art. 151 wird folgender Abs. 60 angefügt:*

„(60) Art. 10 Abs. 1 Z 13 und Art. 102 Abs. 2 in der Fassung des Bundesgesetzes BGBl. I Nr. xxx/2017 treten mit 25. Mai 2018 in Kraft. Gleichzeitig treten in Geltung stehende landesgesetzliche Vorschriften in allgemeinen Angelegenheiten des Schutzes personenbezogener Daten im nicht-automationsunterstützten Datenverkehr außer Kraft.“

FAZIT: Mit dieser Bestimmung werden die – an und für sich bedeutungslosen – landesgesetzlichen Bestimmungen zum Schutz personenbezogener Daten im nicht-automationsunterstützten (manuellen) Datenverkehr außer Kraft gesetzt. Der Bund ist nunmehr allein zuständig für den Datenschutz, sowohl für automationsunterstützt als auch für manuell geführte Datenanwendungen. Betroffen sind von dieser Änderung nachfolgende Landesgesetze:

1. Gesetz vom 7. Juli 2005 über Auskunftspflicht, Datenschutz und Statistik des Landes (Kärntner Informations- und Statistikgesetz – K-ISG)
2. Niederösterreichisches Datenschutzgesetz (NÖ DSG)
3. Landesgesetz über die Auskunftspflicht, den Datenschutz und die Weiterverwendung von Informationen öffentlicher Stellen (Oö. Auskunftspflicht-, Datenschutz- und Informationsweiterverwendungsgesetz)
4. Salzburger Gesetz über Auskunftspflicht, Dokumentenweiterverwendung, Datenschutz, Landesstatistik und Geodateninfrastruktur – ADDSG-Gesetz
5. Gesetz vom 20. März 2001 über den Schutz personenbezogener Daten in nicht automationsunterstützt geführten Dateien (Steiermärkisches Datenschutzgesetz – StDSG)
6. Vorarlberger Landes-Datenschutzgesetz
7. Gesetz über den Schutz personenbezogener Daten (Wiener Datenschutzgesetz – Wr. DSG)
8. Gesetz vom 6. November 2013 über den Schutz personenbezogener Daten im nicht-automationsunterstützten Datenverkehr (Tiroler Datenschutzgesetz 2014 – TDSG 2014)
9. Gesetz vom 30. Juni 2005 über den Schutz personenbezogener Daten bei nicht automationsunterstützt geführten Dateien (Burgenländisches Datenschutzgesetz – Bgld DSG)

Die Umsetzung der DSGVO erfolgt in insgesamt fünf Hauptstücken mit insgesamt 77 Paragraphen und bleibt somit ein „schlankes“ Gesetz.

Artikel 2

Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG)

1. **HAUPTSTÜCK**
GRUNDRECHT AUF DATENSCHUTZ

§ 1 Grundrecht auf Datenschutz

*§ 1. **(Verfassungsbestimmung)** (1) Jede natürliche Person hat Anspruch auf Geheimhaltung der sie betreffenden personenbezogenen Daten, auf Auskunft über die Verarbeitung solcher Daten sowie auf Richtigstellung unrichtiger Daten und auf Löschung unzulässigerweise verarbeiteter Daten.*

(2) Beschränkungen sind nur mit Einwilligung der betroffenen Person, in dessen lebenswichtigem Interesse, im öffentlichen Interesse, und zwar nur aufgrund einer gesetzlichen Grundlage, oder im überwiegenden berechtigten Interesse eines anderen zulässig. Diese Beschränkungen müssen notwendig und verhältnismäßig und, insbesondere im Hinblick auf den Zweck, die verarbeiteten Daten und die Art der Verarbeitung, für die betroffene Person vorhersehbar sein. Im Rahmen hoheitlicher Tätig-

keiten dürfen Beschränkungen nur aufgrund von Gesetzen, die aus den in Art. 8 Abs. 2 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK), BGBl. Nr. 210/1958, genannten Gründen notwendig sind, vorgesehen werden.

(3) Das Grundrecht auf Datenschutz verpflichtet auch Private.

FAZIT: Das Grundrecht auf Datenschutz wurde somit von Österreich neu formuliert. Die Bestimmungen des Art. 6 Abs. 1 f DSGVO werden ausgehebelt und die Bestimmungen des § 8 Abs. 1 Z 4 DSG 2000 aufgenommen (s. untenstehenden Vergleich)! Damit wird die Verwendungsmöglichkeit von personenbezogenen Daten – zB für Big-Data-Anwendungen – sehr eingeengt. Für die Inkraftsetzung dieser Bestimmung ist jedenfalls eine Zweidrittelmehrheit im Parlament erforderlich. Die Frage der EU-Konformität wird noch zu prüfen sein.

Der Schutz juristischer Personen ist im neuen Grundrecht nicht mehr enthalten!

Art. 6 Abs. 1 f DSGVO: *(1) Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:*

[…]

*f) die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, **sofern nicht die Interessen** oder Grundrechte und Grundfreiheiten **der betroffenen Person**, die den Schutz personenbezogener Daten erfordern, **überwiegen**, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.*

§ 8 Abs. 1 Z 4 DSG 2000: *(1) Schutzwürdige Geheimhaltungsinteressen sind bei Verwendung nicht-sensibler Daten dann nicht verletzt, wenn*

[…]

*4. **überwiegende berechtigte Interessen des Auftraggebers** oder eines Dritten die Verwendung erfordern.*

2. HAUPTSTÜCK
DURCHFÜHRUNG DER DATENSCHUTZ-GRUNDVERORDNUNG UND ERGÄNZENDE REGELUNGEN

1. Abschnitt
Allgemeine Bestimmungen

§ 2 Anwendungsbereich

Die Bestimmungen der Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. Nr. L 119 vom 4.5.2016 S. 1, (im Folgenden: DSGVO) und dieses Bundesgesetzes gelten für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen, soweit nicht die spezifischeren Bestimmungen des 3. Hauptstücks dieses Bundesgesetzes vorgehen.

FAZIT: Das DSG gilt somit nicht nur für ganz oder teilweise automatisierte Verarbeitungen personenbezogener Daten, sondern auch für die **nicht automatisierte** Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind. Damit fallen auch manuelle Daten in strukturierter Form, die nach mindestens einem Suchkriterium zugänglich sind, unter die Bestimmungen der DSGVO. So würde zB eine Handkartei, die nach aufsteigenden Nummern oder Namen geordnet ist, als Datei gelten, nicht jedoch Akten oder Aktensammlungen sowie ihre Deckblätter, die nicht nach bestimmten Kriterien strukturiert sind.

§ 3 Durchführungsbestimmung

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 Verar-

beitung der betreffenden personenbezogenen Daten mit der Wirkung nach Art. 18 Abs. 2 DSGVO bis zu diesem Zeitpunkt einzuschränken.

FAZIT: Während Art. 17 Abs. 1 DSGVO eine **unverzügliche Löschung** verlangt, eröffnet diese Bestimmung durch die Übernahme des § 27 Abs. 6 DSG 2000 die – durchaus begrüßenswerte – Möglichkeit, aus wirtschaftlichen oder technischen Gründen die Löschung nur zu bestimmten Zeitpunkten vorzunehmen. Allerdings müssen diese Daten bis zur Löschung gesperrt werden. Ob diese durchaus zu begrüßende Bestimmung EU-konform ist, ist fraglich.

§ 27 Abs. 6 DSG 2000:

(6) Wenn die Löschung oder Richtigstellung von Daten auf ausschließlich automationsunterstützt lesbaren Datenträgern aus Gründen der Wirtschaftlichkeit nur zu bestimmten Zeitpunkten vorgenommen werden kann, sind bis dahin die zu löschenden Daten für den Zugriff zu sperren und die zu berichtigenden Daten mit einer berichtigenden Anmerkung zu versehen.

§ 4 Gemeinsame Bestimmungen zu den Datenschutzbeauftragten

FAZIT: Der Entwurf enthält – einer wesentlichen Forderung der WKÖ entsprechend – keine über die Bestimmungen der DSGVO hinausgehende Verpflichtung, für weitere Fälle verpflichtend einen Datenschutzbeauftragten zu benennen. Somit wird vom österreichischen Gesetzgeber die in Art. 37 Abs. 4 DSGVO enthaltene fakultative Öffnungsklausel nicht in Anspruch genommen. Die Bestimmung legt in Abs. 1 fest, dass die in Art. 38 Abs. 5 DSGVO normierte Geheimhaltungspflicht des Datenschutzbeauftragten auch für dessen Mitarbeiter gilt und enthält in den Erläuterungen eine ergänzende Bestimmung, nämlich die, dass diese Geheimhaltungspflicht **NICHT** gegenüber der DSB gilt! Weiters enthält diese Bestimmung auch ein Aussageverweigerungsrecht des Datenschutzbeauftragten.

§ 5 Datenschutzbeauftragter im öffentlichen Bereich

FAZIT: Enthält zusätzliche Sonderbestimmungen für den DSB im Öffentlichen Bereich. Demnach ist ein Datenschutzbeauftragter im Wirkungsbereich jeden Ministeriums zu benennen. Im Gegensatz zu den Bestimmungen des Art. 7 Abs. 6 DSGVO darf jedoch diese Funktion nicht extern vergeben, sondern nur mit internen Mitarbeitern besetzt werden.

§ 6 Datengeheimnis

(1) Der Verantwortliche, der Auftragsverarbeiter und ihre Mitarbeiter – das sind Arbeitnehmer (Dienstnehmer) und Personen in einem arbeitnehmerähnlichen (dienstnehmerähnlichen) Verhältnis – haben personenbezogene Daten aus Datenverarbeitungen, die ihnen ausschließlich auf Grund ihrer berufsmäßigen Beschäftigung anvertraut wurden oder zugänglich geworden sind, unbeschadet sonstiger gesetzlicher Verschwiegenheitspflichten, geheim zu halten, soweit kein rechtlich zulässiger Grund für eine Übermittlung der anvertrauten oder zugänglich gewordenen personenbezogenen Daten besteht (Datengeheimnis).

(2) Mitarbeiter dürfen personenbezogene Daten nur auf Grund einer ausdrücklichen Anordnung ihres Arbeitgebers (Dienstgebers) übermitteln. Der Verantwortliche und der Auftragsverarbeiter haben, sofern eine solche Verpflichtung ihrer Mitarbeiter nicht schon kraft Gesetzes besteht, diese vertraglich zu verpflichten, personenbezogene Daten aus Datenverarbeitungen nur aufgrund von Anordnungen zu übermitteln und das Datengeheimnis auch nach Beendigung des Arbeitsverhältnisses (Dienstverhältnisses) zum Verantwortlichen oder Auftragsverarbeiter einzuhalten.

(3) Der Verantwortliche und der Auftragsverarbeiter haben die von der Anordnung betroffenen Mitarbeiter über die für sie geltenden Übermittlungsanordnungen und über die Folgen einer Verletzung des Datengeheimnisses zu belehren.

(4) Unbeschadet des verfassungsrechtlichen Weisungsrechts darf einem Mitarbeiter aus der Verweigerung der Befolgung einer Anordnung zur unzulässigen Datenübermittlung kein Nachteil erwachsen.

(5) Ein zugunsten eines Verantwortlichen bestehendes gesetzliches Aussageverweigerungsrecht darf nicht durch die Inanspruchnahme eines für diesen tätigen Auftragsverarbeiter, insbesondere nicht durch die Sicherstellung oder Beschlagnahme von automationsunterstützt verarbeiteten Dokumenten, umgangen werden.

FAZIT: Nachdem die DSGVO keine ausdrückliche Regelung für ein verpflichtendes Datengeheimnis enthält, wurden die Bestimmungen des § 15 DSG 2000 nahezu wörtlich übernommen. Ausdrücklich wird normiert, dass Verantwortliche und Auftragsverarbeiter ihre Mitarbeiter über die für sie geltenden Übermittlungsanordnungen zu belehren haben.

2. Abschnitt
Datenschutzbehörde

§ 7 Einrichtung

FAZIT: Legt die DSB als einzige nationale Aufsichtsbehörde gem. Art. 51 DSGVO fest. Es gibt keine Änderungen im Vergleich zur bisherigen organisatorischen Struktur.

§ 8 Unabhängigkeit

(1) Die Datenschutzbehörde ist eine Dienstbehörde und Personalstelle.

(2) Der Leiter darf für die Dauer seines Amtes keine Tätigkeit ausüben, die

1. *Zweifel an der unabhängigen Ausübung seines Amtes oder seiner Unbefangenheit hervorrufen könnte,*
2. *ihn bei der Erfüllung seiner dienstlichen Aufgaben behindert oder*
3. *wesentliche dienstliche Interessen gefährdet.*

Er ist verpflichtet, Tätigkeiten, die er neben seiner Tätigkeit als Leiter der Datenschutzbehörde ausübt, unverzüglich dem Bundeskanzler zur Kenntnis zu bringen.

(3) Der Bundeskanzler kann sich beim Leiter der Datenschutzbehörde über die Gegenstände der Geschäftsführung unterrichten. Dem ist vom Leiter der Datenschutzbehörde nur insoweit zu entsprechen, als dies nicht der völligen Unabhängigkeit der Aufsichtsbehörde im Sinne von Art. 52 DSGVO widerspricht.

FAZIT: Enthält die Vorgaben für die Unabhängigkeit der DSB. Inwieweit diese durch die Bestimmungen des Abs. 3 vollinhaltlich gegeben ist, ist nach wie vor strittig.

§ 9 Leiter der Datenschutzbehörde

FAZIT: Normiert Bestellung, Anforderungskriterien und Ausschließungsgründe sowie die Enthebung.

§ 10 Aufgaben

(1) Die Datenschutzbehörde berät die Ausschüsse des Nationalrates und des Bundesrates, die Bundesregierung und die Landesregierungen auf deren Ersuchen über legislative und administrative Maßnahmen. Die Datenschutzbehörde ist vor Erlassung von Bundesgesetzen sowie von Verordnungen im Vollzugsbereich des Bundes, die Fragen des Datenschutzes unmittelbar betreffen, anzuhören.

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

(3) Die Datenschutzbehörde hat die nach Art. 57 Abs. 1 lit. p DSGVO festzulegenden Kriterien im Wege einer Verordnung kundzumachen. Sie fungiert zugleich als einzige nationale Akkreditierungsstelle gemäß Art. 43 Abs. 1 lit. a DSGVO.

FAZIT: Die Aufgaben der Datenschutzbehörde (DSB) ergeben sich unmittelbar aus der DSGVO. Nach Art. 35 Abs. 4 und 5 DSGVO hat die DSB im Wege einer Verordnung sowohl eine „Whitelist“ für jene Fälle von Verarbeitungen, für die **KEINE** Datenschutz-Folgenabschätzung durchzuführen ist, sowie eine „Blacklist“ für jene Verarbeitungen, für

die eine Datenschutz-Folgenabschätzung **VERPFLICHTEND** durchzuführen ist, zu erlassen.

Die DSB wird einzige nationale Akkreditierungsstelle für Zertifizierungsstellen, die ein Datenschutzgütesiegel verleihen, und legt auch die Kriterien für diese Stellen fest.

§ 11 Befugnisse

FAZIT: In den Erläuterungen wird ausdrücklich auf die Regelung zum Kumulationsverbot in Art. 83 Abs. 3 DSGVO hingewiesen sowie auf die in Art. 83 iVm ErwG 148 vorgesehene Möglichkeit, anstelle einer Geldbuße eine **Verwarnung** zu erteilen. Konkretisiert wird die Vorgehensweise bei der Überprüfung von Datenverarbeitungen und das Einschau- und Kontrollrecht. Weiters werden die Bestimmungen über die Verschwiegenheitsregelungen der DSB festgelegt. Diese Pflicht besteht auch gegenüber Gerichten und Verwaltungsbehörden, ausgenommen bei Verdacht einer strafbaren Handlung nach den §§ 118a (Widerrechtlicher Zugriff auf ein Computersystem), 119 (Verletzung des Telekommunikationsgeheimnisses), 119a (Missbräuchliches Abfangen von Daten), 126a (Datenbeschädigung), 126b (Störung der Funktionsfähigkeit eines Computersystems), 126c (Missbrauch von Computerprogrammen oder Zugangsdaten), 148a (Betrügerischer Datenverarbeitungsmissbrauch, „Computerbetrug“) oder § 278a (Kriminelle Organisation) sowie von Verbrechen, für die eine Freiheitsstrafe, deren Höchstmaß 5 Jahre übersteigt, vorgesehen ist.

Der DSB obliegt im Rahmen ihrer Zuständigkeit die Verhängung von Geldbußen gegenüber natürlichen und juristischen Personen.

§ 12 Tätigkeitsbericht und Veröffentlichung von Entscheidungen

FAZIT: Konkretisierung der Verpflichtung der DSB zur Erstellung jährlicher Tätigkeitsberichte mit Fälligkeitsdatum 31. März.

3. Abschnitt
Rechtsbehelfe, Haftung und Sanktionen

§ 13 Beschwerde an die Datenschutzbehörde

FAZIT: Enthält das Recht der betroffenen Person auf Beschwerde, wenn sie der Ansicht ist, dass die sie betreffende Verarbeitung gegen die DSGVO oder gegen das erste und zweite Hauptstück des DSG verstößt, sowie die Grundsätze des Verfahrens wie bereits in § 31 Abs. 3, 4, 7 und 8 DSG 2000 vorgesehen. Die DSB erhält außerdem die ausdrückliche Möglichkeit, Amtssachverständige im Verfahren beiziehen zu können.

§ 14 Begleitende Maßnahmen im Beschwerdeverfahren

FAZIT: Legt weitere verfahrensrechtliche Regelungen im Verfahren vor der DSB fest und regelt die Bescheide der DSB auf Basis der bisherigen Bestimmungen des § 38 DSG 2000.

§ 15 Verantwortliche des öffentlichen und des privaten Bereichs

FAZIT: Betrifft den öffentlichen Bereich und behandelt Parteistellung und Rechtsmittellegitimation.

§ 16 Beschwerde an das Bundesverwaltungsgericht

FAZIT: Regelt den Rechtszug von der DSB zum Bundesverwaltungsgericht auf Basis des § 39 DSG 2000.

§ 17 Vertretung von betroffenen Personen

FAZIT: Konkretisiert die Vorgaben des Art. 80 Abs. 1 DSGVO in Bezug auf die Möglichkeit von Verbandsklagen. Im Entwurf ist eine **antragslose** Möglichkeit der Verbandsbeschwerde nicht vorgesehen. Der österreichische Gesetzgeber hat somit die Öffnungsklausel des Art. 80 Abs. 2 DSGVO nicht in Anspruch genommen. Das bedeutet, dass die auf Datenschutz spezialisierten Organisationen („NGOs“) ohne **konkrete Beauftragung** der betroffenen Person weder das Recht haben, eine Beschwerde bei der DSB einzubringen, noch das Klagerecht wahrnehmen können.

§ 18 Haftung und Recht auf Schadenersatz

FAZIT: Konkretisiert die in Art. 82 DSGVO geregelte Haftung sowie das Recht auf materiellen und immateriellen Schadenersatz und legt als zuständiges Gericht die Landesgerichte fest.

§ 19 Allgemeine Bedingungen für die Verhängung von Geldbußen

FAZIT: Enthält die Verhängung von Geldbußen gegen juristische Personen in Analogie zu den Bestimmungen des § 99d BWG. Primär haftet das Unternehmen und nicht derjenige, der das Unternehmen nach außen hin vertritt (Geschäftsführer oder Vorstand). Die DSB kann von der Bestrafung eines Verantwortlichen nach § 9 VStG Abstand nehmen, wenn bereits eine Geldbuße gegen juristische Personen verhängt wurde. Einzelunternehmen hilft diese Bestimmung allerdings nicht!

Die Öffnungsklausel des Art. 83 Abs. 7 DSGVO wird in Anspruch genommen, somit werden gegen Behörden und öffentliche Stellen **KEINE** Geldbußen verhängt.

4. Abschnitt
Datenschutzrat

Einrichtung und Aufgaben

§§ 20 – 24

FAZIT: Enthält die Regelungen zum DSR, die fast zur Gänze von den derzeit geltenden Bestimmungen der §§ 35, 41 bis 44 DSG 2000 übernommen wurden.

5. Abschnitt
Datenverarbeitung zu spezifischen Zwecken

§ 25 Verarbeitung zum Zweck der wissenschaftlichen Forschung und Statistik

FAZIT: Übernimmt die Bestimmungen des § 46 DSG 2000.

§ 26 Zurverfügungstellung von Adressen zur Benachrichtigung und Befragung von betroffenen Personen

FAZIT: Übernimmt die Bestimmungen des § 47 DSG 2000.

§ 27 Freiheit der Meinungsäußerung und Informationsfreiheit

FAZIT: Übernimmt die Bestimmungen des § 48 DSG 2000 für publizistische Tätigkeiten und erweitert die Geltung dieser Bestimmungen auch auf Verarbeitungen zu wissenschaftlichen, künstlerischen und literarischen Zwecken.

§ 28 Verarbeitung personenbezogener Daten im Katastrophenfall

FAZIT: Übernimmt die Bestimmungen des § 48a „Verwendung von Daten im Katastrophenfall“.

§ 29 Verarbeitung personenbezogener Daten im Beschäftigungskontext

Das Arbeitsverfassungsgesetz (ArbVG), BGBl. Nr. 22/1974, ist eine Vorschrift im Sinne des Art. 88 DSGVO. Die dem Betriebsrat nach dem ArbVG zustehenden Befugnisse bleiben unberührt.

FAZIT: Damit ist das Thema eines eigenen Mitarbeiter-Datenschutzgesetzes vorerst vom Tisch.

6. Abschnitt
Bildverarbeitung

§ 30 Zulässigkeit der Bildaufnahme

(1) Eine Bildaufnahme im Sinne dieses Abschnittes bezeichnet die durch Verwendung technischer Einrichtungen zur Bildverarbeitung vorgenommene Feststellung von Ereignissen im öffentlichen oder nicht-öffentlichen Raum zu privaten Zwecken. Zur Bildaufnahme gehören auch dabei mitverarbeitete akustische Informationen. Für eine derartige Bildaufnahme gilt dieser Abschnitt, soweit nicht durch andere Gesetze Besonderes bestimmt ist.

(2) Eine Bildaufnahme ist unter Berücksichtigung der Vorgaben gemäß §§ 32 und 33 zulässig, wenn

1. *sie im lebenswichtigen Interesse einer Person erforderlich ist,*

2. *die betroffene Person zur Verarbeitung ihrer personenbezogenen Daten eingewilligt hat,*
3. *sie durch besondere gesetzliche Bestimmungen angeordnet oder erlaubt ist, oder*
4. *im Einzelfall überwiegende berechtigte Interessen des Verantwortlichen oder eines Dritten bestehen und die Verhältnismäßigkeit gegeben ist.*

(3) Eine Bildaufnahme ist gemäß Abs. 2 Z 4 insbesondere dann zulässig, wenn

1. *sie dem vorbeugenden Schutz von Personen oder Sachen auf privaten Liegenschaften, die ausschließlich vom Verantwortlichen genutzt werden, dient, und räumlich nicht über die Liegenschaft hinausreicht, mit Ausnahme einer zur Zweckerreichung allenfalls unvermeidbaren Einbeziehung öffentlicher Verkehrsflächen,*
2. *sie für den vorbeugenden Schutz von Personen oder Sachen an öffentlich zugänglichen Orten, die dem Hausrecht des Verantwortlichen unterliegen, aufgrund bereits erfolgter Rechtsverletzungen oder eines in der Natur des Ortes liegenden besonderen Gefährdungspotenzials erforderlich ist und kein gelinderes geeignetes Mittel zur Verfügung steht, oder*
3. *sie ein privates Dokumentationsinteresse verfolgt, das nicht auf die identifizierende Erfassung unbeteiligter Personen oder die gezielte Erfassung von Objekten, die sich zur mittelbaren Identifizierung solcher Personen eignen, gerichtet ist.*

(4) Unzulässig ist

1. *eine Bildaufnahme ohne ausdrückliche Einwilligung der betroffenen Person in deren höchstpersönlichen Lebensbereich,*
2. *eine Bildaufnahme zum Zweck der Kontrolle von Arbeitnehmern,*
3. *der automationsunterstützte Abgleich von mittels Bildaufnahmen gewonnenen personenbezogenen Daten mit anderen personenbezogenen Daten oder*
4. *die Auswertung von mittels Bildaufnahmen gewonnenen personenbezogenen Daten anhand von besonderen Kategorien personenbezogener Daten (Art. 9 DSGVO) als Auswahlkriterium.*

FAZIT: Die Bestimmungen schließen nunmehr auch weitere Videoanwendungen wie zB Action-Cams und Wildkameras sowie den Freizeitbereich ein sowie grundsätzlich **ALLE** Bildaufnahmen, so zB auch das Anfertigen von Fotografien zu beruflichen Zwecken. Es gilt der Verhältnismäßigkeitsgrundsatz, wobei die Persönlichkeitsrechte des § 16 ABGB unberührt bleiben. Von den Bestimmungen des Abs. 3 Z 2 sind die in der StMV 2004 enthaltenen Videoüberwachungen für Banken, Juweliere, Handel mit Antiquitäten und Kunstgegenständen, Gold- und Silberschmiede, Trafiken, Tankstellen, bebaute Privatgrundstücke (samt Hauseingang und Garage), Rechenzentren sowie Parkgargen und -plätze umfasst. Entfallen ist die allgemeine Regelung der Auskunft der betroffenen Person. Die Zulässigkeit der Bildverarbeitung iSd DSGVO wird auch weiterhin nicht behandelt.

§ 31 Zulässigkeit der Übermittlung der Bildaufnahme

Im Wege einer zulässigen Bildaufnahme ermittelte personenbezogene Daten dürfen im erforderlichen Ausmaß übermittelt werden, wenn für die Übermittlung eine der Voraussetzungen des § 30 Abs. 2 Z 1 bis 4 gegeben ist. § 30 Abs. 4 gilt sinngemäß.

FAZIT: Bei Bildaufnahmen, die eine strafbare Handlung dokumentieren, dürfen diese auch an die zuständige Behörde oder das zuständige Gericht übermittelt werden.

§ 32 Besondere Datensicherheitsmaßnahmen

(1) Der Verantwortliche hat dem Risiko des Eingriffs angepasste geeignete Datensicherheitsmaßnahmen zu ergreifen und dafür zu sorgen, dass der Zugang zur Bildaufnahme und

eine nachträgliche Veränderung derselben durch Unbefugte ausgeschlossen ist.

(2) Der Verantwortliche hat – außer in den Fällen einer Echtzeitüberwachung – jeden Verarbeitungsvorgang zu protokollieren.

(3) Aufgenommene personenbezogene Daten sind vom Verantwortlichen zu löschen, wenn sie für den Zweck, für den sie ermittelt wurden, nicht mehr benötigt werden und keine andere gesetzlich vorgesehene Aufbewahrungspflicht besteht. Eine länger als 72 Stunden andauernde Aufbewahrung muss verhältnismäßig sein und ist gesondert zu protokollieren und zu begründen.

(4) Die Abs. 1 bis 3 finden keine Anwendung auf Bildaufnahmen nach § 30 Abs. 3 Z 3.

FAZIT: Enthält die Bestimmung, entsprechende Sicherheitsmaßnahmen vorzunehmen (zB. Verschlüsselung) sowie die Protokollierungspflicht jedes Verarbeitungsvorganges. Die Aufbewahrungsdauer ist mit 72 Stunden begrenzt, wobei die Bestimmungen des § 33 Abs. 2 AVG diese kurze Speicherdauer etwas mildern. Jedenfalls wird bei einer längeren Speicherdauer nach den Bestimmungen des Art. 5 Abs. 2 („Rechenschaftspflicht“) eine Begründung zu dokumentieren sein.

§ 33 Kennzeichnung

FAZIT: Wie § 50d DSG 2000 fordert auch § 33 eine entsprechende Kennzeichnung der Bildaufnahme. Dieser kann am wirksamsten mittels eines Piktogramms nach DIN 33450, das auch die Bekanntgabe des Verantwortlichen enthält, nachgekommen werden.

3. 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

§§ 34 bis 68 enthalten die nationalen Umsetzungsbestimmungen zur Richtlinie 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.*

4. HAUPTSTÜCK
BESONDERE STRAFBESTIMMUNGEN

§ 69 Verwaltungsstrafbestimmung

(1) Sofern die Tat nicht einen Tatbestand nach Art. 83 DSGVO verwirklicht oder nach anderen Verwaltungsstrafbestimmungen mit strengerer Strafe bedroht ist, begeht eine Verwaltungsübertretung, die mit Geldstrafe bis zu 50 000 Euro zu ahnden ist, wer

1. *sich vorsätzlich widerrechtlichen Zugang zu einer Datenverarbeitung verschafft oder einen erkennbar widerrechtlichen Zugang vorsätzlich aufrechterhält,*
2. *Daten vorsätzlich in Verletzung des Datengeheimnisses (§ 6) übermittelt, insbesondere Daten, die ihm gemäß §§ 25 oder 26 anvertraut wurden, vorsätzlich für andere unzulässige Zwecke verarbeitet,*
3. *sich unter Vortäuschung falscher Tatsachen vorsätzlich personenbezogene Daten gemäß § 28 verschafft,*
4. *eine Bildverarbeitung entgegen den Bestimmungen des 6. Abschnittes des 2. Hauptstücks betreibt oder*
5. *die Einschau gemäß § 11 Abs. 2 verweigert.*

(2) Der Versuch ist strafbar.

(3) Gegen juristische Personen können bei Verwaltungsübertretung nach Abs. 1 und 2 Geldbußen nach Maßgabe des § 19 verhängt werden.

(4) Die Strafe des Verfalls von Datenträgern und Programmen sowie Bildübertragungs- und Bildaufzeichnungsgeräten kann ausgesprochen werden (§§ 10, 17 und 18 VStG), wenn diese Gegenstände mit einer Verwaltungsübertretung nach Abs. 1 in Zusammenhang stehen.

(5) Die Datenschutzbehörde ist zuständig für Entscheidungen nach Abs. 1 bis 4.

FAZIT: Der österreichische Gesetzgeber nimmt die in Art. 6 Abs. 2 und 3 sowie Art. 23 DSGVO und Kapitel IX der DSGVO iVm ErwG 10 enthaltene Möglichkeit, spezifischere Vorschriften zum Schutz Privater zu erlassen, in Anspruch und sanktioniert bestimmte Verstöße gegen die Bestimmungen des DSG und der DSGVO mit einer Geldstrafe von max. EUR 50.000,00.

§ 70 Datenverarbeitung in Gewinn- oder Schädigungsabsicht

§ 70. Wer mit dem Vorsatz, sich oder einen Dritten dadurch unrechtmäßig zu bereichern, oder mit der Absicht, einen anderen dadurch in seinem von § 1 Abs. 1 gewährleisteten Anspruch zu schädigen, personenbezogene Daten, die ihm ausschließlich auf Grund seiner berufsmäßigen Beschäftigung anvertraut oder zugänglich geworden sind oder die er sich widerrechtlich verschafft hat, selbst benützt, einem anderen zugänglich macht oder veröffentlicht, obwohl der Betroffene an diesen Daten ein schutzwürdiges Geheimhaltungsinteresse hat, ist, wenn die Tat nicht nach einer anderen Bestimmung mit strengerer Strafe bedroht ist, vom Gericht mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bis zu 720 Tagessätzen zu bestrafen.

FAZIT: Mit dieser Bestimmung wurde § 51 DSG 2000 nahezu wortgleich übernommen.

5. HAUPTSTÜCK
SCHLUSSBESTIMMUNGEN

§ 76 Übergangs- und Schlussbestimmungen

(1) *[…]*

(2) Das von der Datenschutzbehörde geführte Datenverarbeitungsregister ist von der Datenschutzbehörde bis zum 31. Dezember 2019 zu Archivzwecken fortzuführen. Es dürfen keine Eintragungen und Änderungen im Datenverarbeitungsregister vorgenommen werden. Registrierungen im Datenverarbeitungsregister werden gegenstandslos. Jedermann kann in das Register Einsicht nehmen. In den Registrierungsakt einschließlich darin allenfalls enthaltener Genehmigungsbescheide ist Einsicht zu gewähren, wenn der Einsichtswerber glaubhaft macht, dass er eine betroffene Person ist, und soweit nicht überwiegende schutzwürdige Geheimhaltungsinteressen des Verantwortlichen (Auftraggebers) oder anderer Personen entgegenstehen.

(3) […]

FAZIT: Mit 25. Mai 2018 wird das Datenvearbeitungsregister (DVR) zwar eingestellt, allerdings bis 31. Dezember 2019 zu Archivzwecken weitergeführt. Das ermöglicht dem Verantwortlichen, auf allfällige Meldungen zurückzugreifen, die im eigenen Firmenarchiv nicht mehr auffindbar sind.

••••