

# Datenschutz im nicht-öffentlichen Bereich in Österreich

*Lukas Feiler / Konrad Lachmayer*

## I. Datenschutz im privaten Bereich

Ausgangspunkt der DSGVO ist der für die Datenverarbeitung Verantwortliche; dieser kann sowohl „natürliche oder juristische Person“<sup>1</sup> als auch „Behörde, Einrichtung oder andere Stelle“<sup>2</sup> sein.<sup>3</sup> Die Festlegung eines privaten Bereichs findet sich in der DSGVO nicht mehr explizit, sondern nur durch die implizite Unterscheidung von Regeln, die entweder an Unternehmen<sup>4</sup> oder an Behörden<sup>5</sup> etc. anknüpfen.

Demgegenüber hält der österreichische Gesetzgeber gem. § 26 DSG die bereits vor der DSGVO bestandene Unterscheidung zwischen öffentlichem und privatem Bereich aufrecht. Der private Bereich wird negativ zum öffentlichen Bereich definiert.<sup>6</sup> In den öffentlichen Bereich fallen i.d.S. gem. § 26 Abs. 1 DSG Verantwortliche, die „in Formen des öffentlichen Rechts eingerichtet sind, insbesondere auch als Organ einer Gebietskörperschaft, oder soweit sie trotz ihrer Einrichtung in Formen des Privatrechts in Vollziehung der Gesetze tätig sind“.

Während für den öffentlichen Bereich zahlreiche nationalstaatliche Sonderregelungen bestehen,<sup>7</sup> gibt es nur eine Bestimmung, die auf die Unterscheidung in Hinblick auf den privaten Bereich Bezug nimmt. § 24 Abs. 5 2. Satz DSG normiert, dass wenn „eine Verletzung einem Verantwortlichen des privaten Bereichs zuzurechnen [ist], so ist diesem [von der Datenschutzbehörde] aufzutragen, den Anträgen des Beschwerdeführers auf Auskunft, Berichtigung, Löschung, Einschränkung oder Datenübertragung in jenem

---

<sup>1</sup> Art. 4 Z. 7 DSGVO.

<sup>2</sup> Ebenda.

<sup>3</sup> Zum Begriff des Verantwortlichen siehe etwa *Hartung*, Art. 4 Z. 7, in Kühling/Buchner (Hrsg.), Kommentar DS-GVO/BDSG<sup>2</sup> (2018); *Eßer*, Art. 4, in Eßer/Kramer/v. Lewinski (Hrsg.), Kommentar DSGVO/BDSG<sup>6</sup> (2018) Rz. 76 ff.

<sup>4</sup> Siehe etwa Art. 37 Abs. 2, Art. 83 Abs. 4 DSGVO.

<sup>5</sup> Siehe etwa Art. 6 Abs. 1, Art. 27 Abs. 2 lit. b, Art. 37 Abs. 1 lit. a DSGVO.

<sup>6</sup> § 26 Abs. 4 DSG: „Die dem Abs. 1 nicht unterliegenden Verantwortlichen [= Verantwortliche des Öffentlichen Bereichs] gelten als Verantwortliche des privaten Bereichs im Sinne dieses Bundesgesetzes“.

<sup>7</sup> Siehe etwa §§ 5 Abs. 3, 5 sowie 10 DSG.

Umfang zu entsprechen, der erforderlich ist, um die festgestellte Rechtsverletzung zu beseitigen“.

Der Datenschutz im privaten Bereich ist konzeptionell aber nicht nur vom öffentlichen Bereich abzugrenzen, sondern auch vom höchstpersönlichen Bereich, der durch Art. 2 Abs. 2 lit. c DSGVO zum Ausdruck kommt.<sup>8</sup> Auch wenn die Anwendung der DSGVO gem. § 4 Abs. 1 DSGVO über den Anwendungsbereich der DSGVO hinaus ausgedehnt werden soll, ist die Haushaltsausnahme in § 4 DSGVO implizit hineinzulesen; der Anwendungsbereich der datenschutzrechtlichen Bestimmungen soll i.d.S. nicht durch die nationale Gesetzgebung auf den höchstpersönlichen Bereich ausgedehnt werden.

Die österreichischen Besonderheiten im privaten Bereich beziehen sich daher nicht explizit auf die Unterscheidung von öffentlichem und privatem Bereich, sondern ergeben sich sachbezogen in unterschiedlichen Verarbeitungsfeldern oder organisatorischen Zusammenhängen, die typischerweise im Bereich relevant werden. I.d.S. werden folgende Themen näher analysiert: Das verfassungsgesetzlich gewährleistete (Grund-)Recht auf Datenschutz gilt in Österreich (noch immer auch) für juristische Personen.<sup>9</sup> Insoweit wird der datenschutzrechtliche Schutzbereich auf juristische Personen ausgeweitet (siehe unter II.). Als ein medial intensiv diskutiertes, aber rechtlich nicht besonders relevantes Thema, erweist sich die Debatte um „Verwarnen statt Strafen“ gem. § 11 DSGVO (III.). Im Fokus stehen sodann in der Praxis besonders relevante Öffnungsklauseln (IV.), insbes. i.Z.m. der Rechtmäßigkeit der Datenverarbeitung (IV.A.), der Ausgestaltung der Betroffenenrechte (IV.B.) sowie dem Arbeitnehmerdatenschutz (IV.C.). Schließlich sind die Perspektiven des Datenschutzrechts im privaten Bereich aufzuzeigen (V.).

## II. Das hartnäckige Grundrecht auf Datenschutz für juristische Personen

In der alten Rechtslage vor Inkrafttreten der DSGVO bestand im österreichischen Datenschutzrecht ein vollumfänglicher Datenschutz für natürli-

---

<sup>8</sup> Vom sachlichen Anwendungsbereich der DSGVO sind i.d.S. Datenverarbeitungen „durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten“ ausgenommen.

<sup>9</sup> Siehe dazu *Heißl* in diesem Band; siehe auch *Lachmayer*, Art. 1, in Knyrim (Hrsg.), *Der DatKomm* (23. Lfg. 2019) Rz. 78 ff.

che und juristische Personen.<sup>10</sup> Das österreichische Grundrecht auf Datenschutz gem. § 1 DSG 2000 sah das Recht auf Geheimhaltung sowie das Grundrecht auf Auskunft, Richtigstellung und Löschung für „Jedermann“ – und damit in der Interpretation des österreichischen Datenschutzrechts – auch einen Schutz von juristischen Personen vor.

Dieser österreichischen Rechtslage entgegengesetzt ist die Konzeption der DSGVO. Nur natürliche Personen sind Betroffene i.S.d. Art. 4 Z 1 DSGVO.<sup>11</sup> Juristische Personen sind nicht nur nicht in der DSGVO geregelt, sondern schon gar nicht vom Anwendungsbereich der DSGVO erfasst.<sup>12</sup> So verbleibt den Mitgliedsstaaten ein Regelungsspielraum, auch die personenbezogenen Daten von juristischen Personen einem Datenschutzregime zu unterwerfen.

In Österreich bestand der Plan, diesen (Daten-)Schutz juristischer Personen in Anpassung an die DSGVO zu ändern. Insoweit wurden auch alle einfachgesetzlichen Bezüge zum Schutz juristischer Personen gestrichen. Im Rahmen des verfassungsgesetzlich gewährleisteten Grundrechts auf Datenschutz blieben aber die entsprechenden Garantien juristischer Personen erhalten. Trotz mehrfacher Anläufe<sup>13</sup> und wechselnder politischen Verhältnisse<sup>14</sup> war es politisch nicht möglich, eine 2/3-Mehrheit im Parlament für die Änderung des Grundrechts zu erreichen.<sup>15</sup> Obwohl diese Angelegenheit (der Änderung des § 1 DSG) selbst nie Zentrum einer politischen Debatte oder gar politischer Gegensätze war, konnte eine entsprechende Novellierung aus jeweils anderen politischen Gründen nicht erzielt werden.<sup>16</sup>

<sup>10</sup> § 4 Z 3 DSG 2000: „jede [...] natürliche oder juristische Person [...]“.

<sup>11</sup> Siehe auch ErwGr 14.

<sup>12</sup> *Lachmayer* in Knyrim zu Art. 1 Rz. 30.

<sup>13</sup> Eine Novellierung des Grundrechts auf Datenschutz wurde zuerst im Kontext des Datenschutz-AnpassungsG 2018, sodann mit dem Datenschutz-DeregulierungsG 2018 und schlussendlich im Rahmen des Bundesgesetzes BGBl. I 2019/14 versucht. Bemerkenswert ist, dass obgleich mit BGBl. I 2019/14 u.a. eine Änderung der verfassungsrechtlichen Kompetenzlage des Datenschutzes – mit Verfassungsmehrheit – erfolgte, eine Novellierung des Grundrechts nicht vorgenommen wurde.

<sup>14</sup> Die Nationalratswahlen 2017 veränderten die Regierungsparteien; während vor den Nationalratswahlen im Oktober 2017 eine Koalition aus SPÖ/ÖVP regierte, besteht seither eine Koalitionsregierung unter ÖVP/FPÖ.

<sup>15</sup> Siehe *Liebel*, Die Rollenverteilung im neuen Datenschutzrecht, Wiener Zeitung v. 26.10.2017 (abrufbar unter: [https://www.wienerzeitung.at/themen\\_channel/recht/recht/925454\\_Die-Rollenverteilung-im-neuen-Datenschutzrecht.html](https://www.wienerzeitung.at/themen_channel/recht/recht/925454_Die-Rollenverteilung-im-neuen-Datenschutzrecht.html)).

<sup>16</sup> Gründe waren etwa das Verweigern einer Verfassungsmehrheit vor den Nationalratswahlen oder Fragen der Klagebefugnis von NGOs im Datenschutzrecht. Vgl. StenProt 190. Sitzung 25. GP 115.

Die rechtliche Konsequenz ist, dass personenbezogene Daten von juristischen Personen weiterhin geschützt bleiben; zumindest auf Ebene des Grundrechts auf Datenschutz.<sup>17</sup> Die verfassungsrechtlichen Konsequenzen für die einfachgesetzlichen Bestimmungen des DSG sind noch unklar; es könnte aber § 4 Abs. 1 DSG somit mit Verfassungswidrigkeit behaftet sein.<sup>18</sup>

Die DSB hat zumindest in Stellungnahmen bereits die Rechtsmeinung vertreten, dass der Datenschutz von juristischen Personen weiterhin im Rahmen des § 1 DSG geschützt wird.<sup>19</sup> Dies ist insbes. auch für ausländische Unternehmen von Relevanz, da auf diese Weise zusätzliche Elemente des Datenschutzes – jenseits der Harmonisierungsbemühungen der DSGVO – entstehen können.

Schließlich besteht aber immer noch die Möglichkeit, dass bei Auftreten ernsthafter Problemstellungen bzw. Divergenzen zur DSGVO durch dieses rechtliche Sonderregime eine Verfassungsmehrheit im Parlament diese Abweichung von der DSGVO beendet.

### III. Verwarnen statt strafen?

§ 11 DSG i.d.F. Datenschutz-AnpassungsG 2018<sup>20</sup> betonte, dass i.Z.m. der Verarbeitung personenbezogener Daten im Beschäftigungskontext, das „Arbeitsverfassungsgesetz [...], soweit es die Verarbeitung personenbezogener Daten regelt, eine Vorschrift im Sinne des Art. 88 DSGVO [ist]. Die dem Betriebsrat nach dem ArbVG zustehenden Befugnisse bleiben unberührt.“<sup>21</sup>

<sup>17</sup> Siehe *Lachmayer* in *Knyrim* zu Art. 1 Rz. 78; vgl. auch *Schmitt*, Facetten des Know-how Schutzes, in *Staudegger/Thiele* (Hrsg.), *Jahrbuch Geistiges Eigentum 2018* (2018) 285 (306 f.).

<sup>18</sup> Siehe *Heißl* in diesem Band.

<sup>19</sup> Siehe dazu etwa die Stellungnahme der DSB zum Entwurf eines Bundesgesetzes mit dem das Telekommunikationsgesetz 2003, das Funkanlagen-Marktüberwachungsgesetz und das Funker-Zeugnisgesetz geändert werden (505/SN-63/ME 26. GP 2): „Dazu ist auszuführen, dass datenschutzrechtliche Rechte gemäß § 1 DSG auch von juristischen Personen begründet werden können. Zwar scheint der Eingriff im Verhältnis zu den Zwecken der Regelungen in einem angemessenen Verhältnis zu stehen, jedoch ist bei der Veröffentlichung von Statistiken jedenfalls auf die Wahrung von § 1 DSG betreffend der Netzbereitsteller-Daten Bedacht zu nehmen, um allfällige Rückschlüsse zu vermeiden.“; dazu auch *Lachmayer* in *Knyrim* zu Art. 1 Rz. 78 ff.

<sup>20</sup> BGBl. I 2017/120.

<sup>21</sup> Siehe zu den arbeitsrechtlichen Besonderheiten sogleich unter IV.C.

Noch vor ihrem Inkrafttreten zum 25.5.2018 wurde diese Bestimmung vollständig durch das sog. Datenschutz-Deregulierungsgesetz 2018<sup>22</sup> geändert.<sup>23</sup>

§ 11 DSGVO i.d.g.F. bezieht sich – im Übrigen auch legislativ systemwidrig innerhalb des DSGVO – auf „Verwarnen durch die Datenschutzbehörde“. <sup>24</sup> I.d.S. hält § 11 DSGVO fest, dass „[d]ie Datenschutzbehörde [...] den Katalog des Art. 83 Abs. 2 bis 6 DSGVO so zur Anwendung bringen [wird], dass die Verhältnismäßigkeit gewahrt wird. Insbesondere bei erstmaligen Verstößen wird die Datenschutzbehörde im Einklang mit Art. 58 DSGVO von ihren Abhilfebefugnissen insbesondere durch Verwarnen Gebrauch machen.“ Erläuternd wurde ausgeführt, dass „[a]uch im Vollzugsbereich des Datenschutzregimes [...] im Einklang mit Art. 58 der DSGVO eine Beratung und eine Verwarnung möglich [...] ist“. Eine Bestrafung erfolgt unter den Abwägungsgründen des Art. 83 DSGVO.“

Während politisch unter dem Slogan „Verwarnen statt Strafen“ eine Entlastung der Wirtschaft proklamiert wurde,<sup>25</sup> ist die rechtliche Bedeutung denkbar gering. Für die DSB ändert § 11 DSGVO nichts. Die Befugnisse der DSB ergeben sich direkt aus der DSGVO. Die Möglichkeit zu verwarnen anstatt zu strafen besteht für die DSB im Rahmen des Verhältnismäßigkeitsprinzips ohnedies. Je nach Erforderlichkeit und Notwendigkeit kann die DSB aber auch andere Abhilfemaßnahmen sofort ergreifen. Sollte es im Einzelfall tatsächlich zu einer rechtlichen Kollision zwischen den Bestimmungen der DSGVO und § 11 DSGVO kommen, ist aufgrund des Anwendungsvorrangs ohnedies nur die DSGVO von der DSB anzuwenden. Die rechtliche Relevanz von § 11 DSGVO ist damit für die Praxis der DSB denkbar gering, wenn nicht sogar überhaupt vernachlässigbar.

<sup>22</sup> BGBl. I 2018/24.

<sup>23</sup> In bemerkenswerter Weise fand die Änderung der Bestimmung in der 2. Lesung des NR statt; der AB beinhaltete noch eine auf den Beschäftigungskontext bezogene Bestimmung. Es wurde also in allerletzter Minute des Gesetzgebungsprozesses der neue Text des § 11 eingefügt (siehe die 21. Sitzung des NR v. 20.4.2018, 26. GP, 28 ff.).

<sup>24</sup> Zur Ausgestaltung der Datenschutzbehörde siehe in diesem Band *Ennöckl/Lachmayer*.

<sup>25</sup> Siehe etwa *Markus Dörfler*, Wie man dem Datenschutz-Krokodil nicht die Zähne zieht, *derStandard* v. 6.5.2018 (abrufbar unter: <https://derstandard.at/2000079201077/DatenschutzderegulierungWie-man-dem-Krokodil-nicht-die-Zaehne-zieht>); *Petra Tempfer*, Die österreichische Lösung beim Datenschutz, *Wiener Zeitung* v. 24.5.2018 (abrufbar unter: [https://www.wienerzeitung.at/themen\\_channel/recht/recht/966773\\_Die-oesterreichische-Loesung-beim-Datenschutz.html](https://www.wienerzeitung.at/themen_channel/recht/recht/966773_Die-oesterreichische-Loesung-beim-Datenschutz.html)).

## IV. In der Praxis besonders relevante Öffnungsklauseln

### A. Öffnungsklauseln zur Rechtmäßigkeit der Datenverarbeitung

Die DSGVO sieht viele Öffnungsklauseln vor, von denen der österreichische Gesetzgeber nur die wenigsten aufgegriffen hat. Manche davon sind für den privaten Bereich von Relevanz. An dieser Stelle sollen insbes. die Altersgrenze für die Einwilligung von Jugendlichen gemäß Art. 8 DSGVO, die Verwendung von strafrechtlich relevanten Daten gemäß Art. 10 DSGVO, die Forschungsprivilegierung gem. § 7 DSG sowie FOG und die Regeln zur Bildverarbeitung gem. § 12 f. DSG hervorgehoben werden.<sup>26</sup>

#### – Altersgrenze für Einwilligung eines Jugendlichen gem. Art. 8 DSGVO

Art. 8 DSGVO sieht – auf unionsrechtlicher Ebene erstmals – Bedingungen für die Einwilligung i.S.d. Art. 6 Abs. 1 lit. a DSGVO für Kinder vor. Allerdings kommt es zu keiner allgemeinen Regulierung der Verarbeitung von personenbezogenen Daten, sondern nur eingeschränkt für Angebote „von Diensten der Informationsgesellschaft, [...] [die] einem Kind direkt gemacht [...] [werden]“. Als allgemeine Altersgrenze wird die Vollendung des sechzehnten Lebensjahrs vorgesehen; in diesen Fällen ist die Verarbeitung nur rechtmäßig, wenn die „Träger der elterlichen Verantwortung für das Kind“ einwilligen. Von diesem Grundsatz kann aber gem. Art. 8 Abs. 1 UAbs. 2 DSGVO durch Rechtsvorschriften der Mitgliedsstaaten abgewichen werden, um „eine niedrigere Altersgrenze vorzusehen, die jedoch nicht unter dem vollendeten dreizehnten Lebensjahr liegen darf“.

Der österreichische Gesetzgeber hat von dieser Möglichkeit Gebrauch gemacht und die *Altersgrenze* für die Einwilligung eines Kindes gem. § 4 Abs. 4 DSG bis zur Vollendung des 14. Lebensjahrs festgelegt. Zahlreiche Anknüpfungspunkte, wie die strafrechtliche Verantwortlichkeit, der Wechsel von Schulformen und die zivilrechtliche Unterscheidung zwischen mündigen und unmündigen Minderjährigen knüpfen an das vollendete 14. Lebensjahr an.

I.S.d. Art. 8 DSGVO knüpft auch § 4 Abs. 4 DSG an das „Angebot von Diensten der Informationsgesellschaft“ an. Es verbleibt daher sowohl auf nationaler als auch auf unionsrechtlicher Ebene eine Lücke in Hinblick auf die Datenverarbeitungen, die nicht im Kontext von Diensten der Informations-

<sup>26</sup> Zur Medienprivilegierung siehe den Beitrag von *Jahnel* in diesem Band.

gesellschaft erfolgen.<sup>27</sup> Es ist allerdings nicht davon auszugehen, dass in jenen Fällen, in denen es sich nicht um Dienste der Informationsgesellschaft handelt, die Einwilligung durch Kinder selbst getätigt werden kann. Es ist daher vielmehr von einer gleichlaufenden Behandlung auszugehen. Der Richtwert bleibt damit in Österreich – im Gegensatz zu dem in Deutschland vorgesehenen 16. Lebensjahr<sup>28</sup> – das 14. Lebensjahr.

– Strafrechtlich relevante Daten gem. Art. 10 DSGVO

Gem. Art. 10 DSGVO dürfen personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten sowie damit zusammenhängende Sicherungsmaßnahmen nur unter bestimmten Bedingungen verarbeitet werden. Dazu zählen neben der (selbstverständlichen) Rechtmäßigkeit der Verarbeitung gem. Art. 6 Abs. 1 die behördliche Aufsicht oder eine explizite rechtliche Grundlage der Mitgliedstaaten, die geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen vorsieht.

Die Regelung des Art. 10 DSGVO ist in Abgrenzung der DSRL-PJZS zu begreifen, die die behördliche Verarbeitung von personenbezogenen Daten zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung regelt. Damit ist insbes. die Datenverarbeitung von personenbezogenen Strafdaten durch Private betroffen.

Eine mitgliedstaatliche Regelung, die auf Art. 10 DSGVO aufbaut, findet sich in § 4 Abs. 3 DSG. Diese Bestimmung bezieht nicht nur gerichtliche Straftaten mit ein, sondern auch sog. Verwaltungsstraftaten, die den Ordnungswidrigkeiten im deutschen Recht entsprechen. Als nationale Bedingungen werden konkretisierend zu Art. 10 DSGVO folgende zwei Alternativen der Rechtmäßigkeit genannt:

- Bestehen einer ausdrücklichen gesetzlichen Ermächtigung oder Verpflichtung zur Verarbeitung solcher Daten;
- sich die Zulässigkeit der Datenverarbeitung „aus gesetzlichen Sorgfaltspflichten ergibt oder die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten gemäß Art. 6 Abs. 1 lit. f DSGVO erforderlich ist, und die Art und Weise, in der die Datenver-

<sup>27</sup> Siehe *Kastelitz*, Art. 8, in Knyirm (Hrsg.), *Der DatKomm* (2018) Rz. 5: „offen bleibt [...], was außerhalb des ‚Online-Kontexts‘ gilt“.

<sup>28</sup> Vgl. *Heckmann/Paschke*, Art. 8, in Ehmman/Selmayr (Hrsg.), *DS-GVO*<sup>2</sup> (2018) Rz. 42; *Kampert*, Art. 8, in Sydow (Hrsg.), *DSGVO*<sup>2</sup> (2018) Rz. 12.

arbeitung vorgenommen wird, die Wahrung der Interessen der betroffenen Person nach der DSGVO und diesem Bundesgesetz gewährleistet“.<sup>29</sup>

§ 4 Abs. 3 DSG erweist sich damit nicht als eine Bestimmung i.S.d. Art. 10 DSGVO, da dieser eben keine konkrete gesetzliche Ermächtigung vorsieht, sondern selbst wiederum auf andere gesetzliche Ermächtigungen verweist. § 4 Abs. 3 DSG ist damit vielmehr eine Wiederholung von Art. 10 DSGVO. Die einzige Funktion des § 4 Abs. 3 DSG könnte sodann vielmehr darin bestehen, dass bestimmte Rechtmäßigkeitstatbestände des Art. 6 Abs. 1 DSGVO ausgeschlossen werden sollten, wie etwa die Verarbeitung aufgrund einer Einwilligung gem. Art. 6 Abs. 1 lit. a DSGVO oder aufgrund eines Vertrages gem. Art. 6 Abs. 1 lit. b DSGVO. So verstanden widerspricht § 4 Abs. 3 DSG der ersten der zwei Alternativen gem. Art. 10 DSGVO. Wie in Art. 10 DSGVO geforderte, geeignete Garantien finden sich ebenso wenig wie Regelungen zur behördlichen Aufsicht.<sup>30</sup>

Insgesamt erweist sich § 4 Abs. 3 DSG damit – weil die Bestimmung eben keine konkretisierenden Regelungen für die konkrete Datenverarbeitung über strafrechtliche Daten enthält – als eine im Lichte der Vorgaben des Art. 10 DSGVO problematische Regelung.

– Forschungsprivilegierung gem. § 7 DSG<sup>31</sup>

Art. 89 Abs. 2 DSGVO ermöglicht Ausnahmen von den Rechten betroffener Personen, wenn es sich um Datenverarbeitungen zu wissenschaftlichen Forschungszwecken<sup>32</sup> handelt. § 7 DSG greift u.a. das Thema der Verarbeitung zu Forschungszwecken auf, bezieht sich aber nicht auf die Ausnahmen von Rechten Betroffener gem. Art. 89 Abs. 2 DSGVO. Es handelt sich bei dieser Bestimmung vielmehr um eine Konkretisierung i.S.d. Art. 6 Abs. 2 und 3 DSGVO, unter welchen Umständen Verantwortliche personenbezogene Daten zu wissenschaftlichen Zwecken verarbeiten dürfen.

<sup>29</sup> § 4 Abs. 3 DSG.

<sup>30</sup> Vgl. *Kunnert*, § 4 DSG, in Bresich et al. (Hrsg.), DSG Kommentar (2018) Rz. 17, der infrage stellt, inwieweit die „abstrakte Formulierung in § 4 Abs. 3 Z 2 tatsächlich als Garantie i.S.d. Art. 10 Abs. 1 DSGVO gewertet werden kann“.

<sup>31</sup> Siehe dazu näher *Lachmayer/Souhrada-Kirchmayer*, Datenschutzrecht in der wissenschaftlichen Forschung, zfhr 2018, 153 (155 f.).

<sup>32</sup> Art. 89 DSGVO nennt neben den wissenschaftlichen Forschungszwecken als weitere Zwecke historische Forschungszwecke und statistische Zwecke.

Die Datenverarbeitungen haben dabei insbes. im öffentlichen Interesse liegenden Forschungszwecken zu dienen, müssen aber nicht zwingend durch staatliche Stellen – insbes. staatliche Universitäten – erbracht werden. Es werden daher auch private Forschungseinrichtungen, Unternehmen bzw. private ForscherInnen von § 7 DSGVO erfasst.

Neben der eingeschränkten Forschungsprivilegierung des § 7 DSGVO bestehen aber darüber hinaus im Rahmen des Forschungsorganisationsgesetzes (FOG)<sup>33</sup> parallel<sup>34</sup> breitflächige Erleichterungen der Datenverarbeitungen auch für private Forschungseinrichtungen und Unternehmen, die zu Forschungszwecken Daten verarbeiten. Insbes. sieht § 2d FOG vor, dass unter Einhaltung zahlreicher technischer und organisatorischer Maßnahmen ohne Einwilligung der betroffenen Personen personenbezogene Daten breitflächig verarbeitet werden können. So sieht das FOG auch Einschränkungen der Betroffenenrechte i.S.d. Art. 89 Abs. 2 DSGVO vor.<sup>35</sup> Fraglich bleibt, inwieweit die weitgehenden Regelungen des FOG den Prinzipien des Datenschutzrechts der DSGVO widersprechen.<sup>36</sup>

#### – § 12 f. DSGVO Bildverarbeitung

Ein nationalstaatlicher Regelungsbereich gem. § 12 f. DSGVO bezieht sich auf Bildverarbeitungen. Dieser baut nicht auf spezifischen Regelungen der DSGVO auf, sondern setzt vielmehr die in Österreich vor Erlassung der DSGVO bestehenden spezifischen Regelungen im DSGVO fort.<sup>37</sup> Diese Regelungen fokussieren den privaten Bereich und schließen die hoheitliche Bildverarbeitung, die eigenen Regelungen unterliegt, explizit aus. Konkret geht es gem. § 12 Abs. 1 DSGVO um „die durch Verwendung technischer Einrichtungen zur Bildverarbeitung vorgenommene Feststellung von Ereignissen im öffentlichen oder nicht-öffentlichen Raum zu privaten Zwecken“, wobei damit eben jene Datenverarbeitungen im Rahmen der Haushaltsausnahme nicht gemeint sind.<sup>38</sup>

<sup>33</sup> BGBl. 1981/341.

<sup>34</sup> Es liegt kein Fall der Derogation von § 7 DSGVO durch eine *lex specialis* vor; siehe dazu *Lachmayer/Soubrada-Kirchmayer*, zfhr 2018, 157.

<sup>35</sup> Siehe § 2d Abs. 6 FOG.

<sup>36</sup> *Kunnert*, § 7 DSGVO, in Bresich et al. (Hrsg.), DSGVO Kommentar (2018) Rz. 9; *Lachmayer/Soubrada-Kirchmayer*, zfhr 2018, 157 f.

<sup>37</sup> *König*, § 12 DSGVO, in Gantschacher/Jelinek/Schmidl/Spanberger (Hrsg.), DSGVO Kommentar (2018) Rz. 1.

<sup>38</sup> ErläutRV 1664 BlgNR 25. GP 14.

Für die Bildaufnahmen, die sich im Übrigen auch auf „mitverarbeitete akustische Informationen“ beziehen, sind eigenständige Rechtmäßigkeitskriterien vorgesehen, die den Regelungsinhalten vor Erlassung der DSGVO entsprechen. Darüber hinaus werden gem. § 13 DSG besondere Datensicherheits- und Kennzeichnungsmaßnahmen vorgesehen.

Die unionsrechtliche Zulässigkeit dieser Regelungen ist allerdings höchst fragwürdig, da die Berufung auf Art. 6 Abs. 2 und 3 DSGVO zur Legitimation der § 12 f. DSG nicht überzeugend herangezogen werden kann.<sup>39</sup> Der bei Berücksichtigung des Anwendungsvorrangs verbleibende Anwendungsbereich der nationalstaatlichen Regelung erweist sich als minimal.<sup>40</sup>

#### – Zusammenfassung

Die österreichische Art und Weise des Aufgreifens von Öffnungsklauseln steht potenziell im Konflikt mit den Vorgaben der DSGVO. Einerseits werden bestehende datenschutzrechtliche Konzepte weitergeführt, ohne dass auf die DSGVO Rücksicht genommen wird (Bsp.: Bildverarbeitung); zumindest aber werden die Grenzen der Öffnungsklauseln stark ausgereizt (Bsp.: Forschungsprivilegierung i.S.d. FOG). Andererseits werden unionsrechtliche Bestimmungen so wiederholt, dass die von der DSGVO geforderten Konkretisierungen gerade nicht enthalten sind (Bsp.: Strafrechtliche Datenverarbeitungen, Medienprivilegierung<sup>41</sup>).

Neben den allgemeinen Konkretisierungen im Rahmen des DSG bestehen aber zahlreiche Anpassungen in den vielfältigen Sachmaterien; in Form von zwei Materien-Datenschutz-Anpassungsgesetzen<sup>42</sup> wurden großflächige Änderungen vorgenommen, die noch einer Analyse bedürfen.<sup>43</sup>

Insgesamt besteht somit noch erheblicher Anpassungsbedarf bei den nationalen Normen zur Umsetzung der DSGVO-Öffnungsklauseln.

<sup>39</sup> Siehe dazu ausführlich *Müllner/Wieser*, §§ 12 f DSG – Kein Spielraum für Beharrlichkeit, jusIT 2019 (in Druck).

<sup>40</sup> Ebenda.

<sup>41</sup> Siehe dazu den Beitrag von *Jahnel* in diesem Band.

<sup>42</sup> BGBl. I 2018/32 und BGBl. I 2018/37.

<sup>43</sup> Diese kann im Rahmen dieses Beitrages nicht erfolgen.

## B. Ausgestaltung der Betroffenenrechte

Im Kontext der Betroffenenrechte bestehen nationalstaatliche Ausgestaltungen. Diese wurden in Österreich auf unterschiedliche Weise beschränkt. Implizit erklärt § 4 Abs. 2 DSG, dass anstatt einer unverzüglichen Berichtigung oder Löschung, wenn „diese aus wirtschaftlichen oder technischen Gründen nur zu bestimmten Zeitpunkten vorgenommen werden kann“, eine Einschränkung i.S.d. Art. 18 DSGVO ausreichend ist.<sup>44</sup> Unter Berufung auf vor der DSGVO bestandene Regelungen wurde die Bestimmung im parlamentarischen Prozess hineinreklamiert.<sup>45</sup>

Eine Beschränkung der Betroffenenrechte ist gem. Art. 23 DSGVO möglich; dies allerdings nur unter den in dieser Bestimmung genannten Voraussetzungen. Diese werden bei § 4 Abs. 2 DSG dadurch erfüllt, dass die Norm den Schutz der Rechte und Freiheiten anderer Personen sicherstellt.<sup>46</sup>

Durch das Datenschutz-DeregulierungsG 2018 wurde in § 4 Abs 6 DSG überdies das Recht auf Auskunft der betroffenen Person gemäß Art. 15 DSGVO insoweit beschränkt, als „durch die Erteilung dieser Auskunft ein Geschäfts- oder Betriebsgeheimnis des Verantwortlichen bzw. Dritter gefährdet würde“.<sup>47</sup> Dies ist auch zweckmäßig, da Geschäfts- oder Betriebsgeheim-

---

<sup>44</sup> *Haidinger*, Art. 18, in Knyrim (Hrsg.), *Der DatKomm* (2018) Rz. 20: „Diesfalls sind die Daten bis dahin mit der Wirkung nach Art. 18 Abs. 2 einzuschränken, womit allerdings ebenfalls datentechnische Herausforderungen verbunden sind. Entsprechende organisatorische Umgehungsmaßnahmen sind daher zu empfehlen.“

<sup>45</sup> Siehe die Erl zu § 4 DSG (AB 1761 BlgNR 25. GP 4): „Im DSG 2000 ist derzeit vorgesehen, dass dann, wenn die Löschung oder Richtigstellung von personenbezogenen Daten auf ausschließlich automationsunterstützt lesbaren Datenträgern aus Gründen der Wirtschaftlichkeit nur zu bestimmten Zeitpunkten vorgenommen werden kann, die zu löschenden personenbezogenen Daten für den Zugriff zu sperren und die zu berichtigenden personenbezogenen Daten mit einer berichtigenden Anmerkung zu versehen sind (§ 27 Abs. 6 DSG 2000). Die DSGVO trifft für einen solchen Fall keine ausdrückliche Vorsorge. Insbesondere bei einer etwa aus Sicherheitsgründen weit verteilten Speicherung von personenbezogenen Daten kann es sich im Einzelfall als schwierig erweisen, einzelne Datensätze sofort aus sämtlichen Kopien zu entfernen. In diesem Lichte erscheint die Beibehaltung einer technikneutral formulierten, adaptierten Fassung des bisherigen § 27 Abs. 6 DSG 2000 sachgerecht. Unter diese Bestimmung sind auch Konstellationen im Zusammenhang mit der Verwendung von Backup-Datensicherungen und Löschungsrouitinen zu subsumieren.“

<sup>46</sup> So auch *Kunnert* in Bresich et al. zu § 4 Rz. 12.

<sup>47</sup> Siehe *Kunnert* in Bresich et al. zu § 4 Rz. 26 f.: keinesfalls durch § 4 Abs. 6 gedeckt sind Auskunftsverweigerungen unter Pauschalverweis auf Geschäfts- und Betriebsgeheimnisse; *Haidinger*, Art. 15, in Knyrim (Hrsg.), *Der DatKomm* (2018) Rz. 51.

nisse einerseits selbst personenbezogene Daten darstellen können, andererseits aber in diesen Fällen jedenfalls ein schützenswertes Geheimhaltungsinteresse des Verantwortlichen besteht.<sup>48</sup>

§ 4 Abs. 6 DSGVO entspricht Art. 23 Abs. 1 lit. i DSGVO, weil Geschäfts- und Betriebsgeheimnisse den Schutz der Rechte und Freiheiten „anderer Personen“ betreffen, die auch mit dem Verantwortlichen ident sein dürfen.<sup>49</sup> § 4 Abs. 6 DSGVO ist unionsrechtskonform jedenfalls so zu interpretieren, dass es sich nicht um eine absolute Beschränkung handelt, sondern i.S.d. Verhältnismäßigkeitsprinzips eine Abwägung zu erfolgen hat.<sup>50</sup>

Zu politischen Diskussionen führte im Rahmen der Datenschutzanpassungen die Streichung der Vertretungsbefugnis durch Vereine (NGOs) hinsichtlich der Schadenersatzansprüche gem. Art. 80 Abs. 1 DSGVO. So wurde durch die Novelle des Datenschutz-Deregulierungsgesetz 2018 die entsprechende Bestimmung gem. § 28 DSGVO i.d.F. Datenschutz-Anpassungsgesetz 2018<sup>51</sup> wieder entfernt. Die Streichung durch die BReg führte zur Weigerung der Opposition, das Grundrecht auf Datenschutz – wie oben besprochen<sup>52</sup> – zu ändern.

Bei der gerichtlichen Geltendmachung von Betroffenenrechten gem. Art. 79 DSGVO besteht im Rahmen der österreichischen Rechtsordnung eine unionsrechtlich problematische Einschränkung. Während das Unionsrecht das Recht auf gerichtlichen Rechtsbehelf „unbeschadet eines verfügba-

<sup>48</sup> Siehe dazu die österreichische Rsp. bereits vor der DSGVO (OGH 25.10.2016, 4 Ob 165/16t, Ticketsysteme = ZIIR 2017/78 (*Kralik*) = AnwBl 2017/8477, 104 (*Mahr/Swoboda*) = ecolex 2017/34, 53 (*Horak*) = jusIT 2017/31, 61 (*Staudegger*) = ÖBl 2017/37, 136 (*Tonninger*).

<sup>49</sup> Unter einer „anderen Person“ ist auch der Verantwortliche zu verstehen. *Herbst*, Art. 23, in Eßer/Kramer/v. Lewinski (Hrsg.), Kommentar DSGVO/BDSG<sup>6</sup> (2018) Rz. 19; siehe auch *Bäcker*, Art. 23, in Kühling/Buchner (Hrsg.), Kommentar DS-GVO/BDSG<sup>2</sup> (2018) Rz. 32.

<sup>50</sup> *Bäcker* in Kühling/Buchner zu Art. 23 Rz. 32: rein wirtschaftliche Interessen können zur Beschränkung nicht herangezogen werden, insoweit sie nicht einen besonderen rechtlichen Schutz genießen.

<sup>51</sup> „Die betroffene Person hat das Recht, eine Einrichtung, Organisationen oder Vereinigung ohne Gewinnerzielungsabsicht, die ordnungsgemäß gegründet ist, deren satzungsmäßige Ziele im öffentlichem Interesse liegen und die im Bereich des Schutzes der Rechte und Freiheiten von betroffenen Personen in Bezug auf den Schutz ihrer personenbezogenen Daten tätig ist, zu beauftragen, in ihrem Namen eine Beschwerde einzureichen, in ihrem Namen die in den §§ 24 bis 27 genannten Rechte wahrzunehmen und das Recht auf Schadenersatz gemäß § 29 in Anspruch zu nehmen“.

<sup>52</sup> Siehe unter II.

ren verwaltungsrechtlichen oder außergerichtlichen Rechtsbehelfs“ einfordert, ist aus den einschlägigen Regelungen des DSGVO nur im Rahmen des Schadenersatzanspruches i.S.d. § 29 Abs. 2 DSGVO ein unmittelbarer Rechtsschutz gegeben; dieser bezieht sich aber auf Art. 82 DSGVO. Es ist daher vielmehr auf Basis des Anwendungsvorrangs der DSGVO davon auszugehen, dass auch ein unmittelbarer Rechtsschutz direkt auf Art. 79 DSGVO gestützt werden kann.<sup>53</sup>

### C. Datengeheimnis und Arbeitnehmerdatenschutzrecht

Bevor auf die Spezifika des Arbeitnehmerdatenschutzrechts eingegangen wird, ist das Datengeheimnis gem. § 6 DSGVO zu erwähnen. Die Bestimmung verpflichtet Arbeitnehmer „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)“. Eine verwandte Vorschrift findet sich in Art. 32 Abs. 4 DSGVO, wonach der Verantwortliche sicherzustellen hat, dass ihm „unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet“.

Zum Arbeitnehmerdatenschutz zählen hingegen alle Bestimmungen zum Schutz von ArbeitnehmerInnen gegenüber der Erfassung von personenbezogenen Daten durch ArbeitgeberInnen. Art. 88 DSGVO gibt den Mitgliedstaaten die Möglichkeit, „durch Rechtsvorschriften oder durch Kollektivvereinbarungen spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigendaten im Beschäftigungskontext [...]“ vorzusehen.

Wie bereits erwähnt wurde durch das Datenschutz-DeregulierungsG 2018 der Bezug zum Arbeitnehmerdatenschutz in § 11 DSGVO a.F. gestrichen.<sup>54</sup> Das bereits vor Geltung der DSGVO im Arbeitsverfassungsrecht bestehende Datenschutzrecht lebt aber fort. Damit sind die bestehenden Informationspflichten

<sup>53</sup> Siehe dazu auch *Enmöckl/Lachmayer* in diesem Band.

<sup>54</sup> Siehe i.d.Z. *Brodil*, Datenschutz und Arbeitsrecht – Was ändert sich durch die Datenschutz-Grundverordnung?, DRdA 2018, 463 (470 f.).

ten gegenüber dem Betriebsrat (§ 91 Abs. 2 ArbVG), die Einsichtsrechte des Betriebsrats (§ 89 ArbVG), die erforderlichen Betriebsvereinbarungen (§§ 96, 96a ArbVG) weiterhin relevant.<sup>55</sup> Darüber hinaus bleiben individualarbeitsrechtliche Einwilligungserfordernisse bestehen. Dazu zählt die praktisch bedeutsame Vorschrift gem. § 10 AVRAG, wonach Kontrollmaßnahmen, die die Menschenwürde berühren und in Betrieben ohne Betriebsrat implementiert werden, weiterhin die (arbeitsrechtliche) Einwilligung des Arbeitnehmers voraussetzen.

Insgesamt verändern sich die spezifischen Vorgaben im Arbeitnehmerdatenschutz nicht. Allerdings sind die Anforderungen an die Unternehmen, den Arbeitnehmerdatenschutz professionell zu handhaben, durch die DSGVO insgesamt gestiegen und die Sanktionsmöglichkeiten wesentlich massiver als bisher ausgestaltet.

## V. Ausblick

Die österreichische Datenschutz-Anpassung ist – wie dieser kurze Überblick gezeigt hat – durchaus vom Bemühen getragen, im privaten Bereich gewisse Spielräume zu eröffnen und damit den Datenschutz zumindest punktuell zu begrenzen. Die diesbezügliche legistische Vorgangsweise erweist sich nur zum Teil als geglückt, da die Regelungen oftmals einer datenschutzrechtlichen Logik vor Erlassung der DSGVO entsprechen oder sich nicht an den Öffnungsklauseln der DSGVO orientieren. Es wird daher in den nächsten Jahren noch ein Prozess der Adaptierung der nationalen Anpassung erforderlich werden, um den Vorgaben der DSGVO zu entsprechen.

---

<sup>55</sup> Vgl. *Brodil*, DRdA 2018, 471 f., der die Spezifität der §§ 96, 96a ArbVG in Hinblick auf Art. 88 DSGVO problematisiert.