ARGE DATEN
*ARGE DATEN - Österreichische Gesellschaft für Datenschutz*

An die
Parlamentsdirektion
Begutachtungsverfahren

1010 Wien

Wien, 23. Juni 2017

Betreff: Zeichen: BKA-810.026/0019-V/3/2017
Stellungnahme zum Entwurf eines Bundesgesetzes, mit dem das Bundes-Verfassungsgesetz geändert, das Datenschutzgesetz erlassen und das Datenschutzgesetz 2000 aufgehoben wird (Datenschutz-Anpassungsgesetz 2018, DSG 2018)

In der Anlage finden Sie die Stellungnahme der
**ARGE DATEN - Österreichische Gesellschaft für Datenschutz**
mit dem dringenden Ersuchen um Kenntnisnahme und Berücksichtigung.

Für allfällige Fragen stehen wir gerne zur Verfügung.

Mit vorzüglicher Hochachtung

*elektronisch erstellt*
Dr. Hans G. Zeger (Obmann) Mag. Philipp Hochstöger

**Anlage:**
Stellungnahme elektronisch übermittelt
(*begutachtungsverfahren@parlament.gv.at*)

Alle Stellungnahmen werden unter ftp://ftp.freenet.at/privacy/gesetze veröffentlicht.

*ARGE DATEN - Österr. Gesellschaft für Datenschutz http://www.argedaten.at info@argedaten.at ☎ +43/676/9107032, Fax +43/1/5320974*
*Vereins- und Rechnungsadresse: A-1160 Wien, Redtenbacherg. 20 DVR 0530794ZVR 774004629 UID ATU 56627966 Gerichtsstand Wien*
***Geschäfts- und Zustelladresse: A-1010 Wien, Vorlaufstraße 5/6***
*DB RECHT / STELL / Datenschutz-Anpassungsgesetz 2018*

# 1. Einleitung

Die Datenschutz-Grundverordnung (DSGVO) kann als Hybrid zwischen Richtlinie und Verordnung bezeichnet werden.[1] Der österreichische Gesetzgeber muss tätig werden. Man spricht in diesem Zusammenhang auch von „obligatorischen" Öffnungsklauseln. Weiters schafft die DSGVO die Möglichkeit für den österreichischen Gesetzgeber im Rahmen der Regelungsspielräume selbst gestaltend tätig zu werden. Da hier jedoch keine Pflicht für Mitgliedstaaten besteht, spricht man von „fakultativen" Öffnungsklauseln.

Sowohl für die Umsetzung obligatorischer als auch fakultativer Öffnungsklauseln gilt: Leitprinzip der mitgliedstaatlichen Umsetzung der DSGVO muss immer – diesen Maßstab setzt auch der Begutachtungstext der ARGE DATEN an - die Schaffung von Rechtssicherheit sein. Konflikte mit europäischen Bestimmungen müssen vermieden werden, um eine Nichtanwendung der Regelungen des Datenschutz-Anpassungsgesetzes 2018 (DSG 2018) möglichst hintanzuhalten (sog. „Anwendungsvorrang des Unionsrechts"). Den österreichischen Unternehmen müssen klare Regelungen in die Hand gegeben werden, damit die verbleibende Zeit bis zum 25.5.2018 zur Implementierung der Verpflichtungen genutzt werden kann.

Die Stellungnahme befasst sich vorwiegend mit der Vereinbarkeit der Bestimmungen des DSG 2018 mit der DSGVO. Auch wenn im vorliegenden Entwurf von den Öffnungsklauseln nur sehr sparsam Gebrauch gemacht wird, ist die Tendenz zur Übernahme von Bestimmungen aus der alten Rechtslage (DSG 2000) in den vorliegenden Entwurf klar erkennbar. Diese Vorgangsweise wird von der ARGE DATEN zwar nicht per se als problematisch angesehen, führt jedoch – wie noch zu zeigen ist – zu einem Konflikt mit den europäischen Vorgaben. Soweit Bestimmungen aus dem DSG 2000 in das neue Datenschutzrecht übernommen werden, müssen diese mit der DSGVO vereinbar sein. In dieser Hinsicht besteht noch Anpassungsbedarf.

# 2. Scoring weiterhin ungeregelt

Die DSGVO steht für einen verbesserten Datenschutz für betroffene Bürger. Ein europaweiter Rechtsrahmen kann jedoch unmöglich alle schützenswerten Sachverhalte in den Mitgliedstaaten abschließend regeln. So führt in Österreich seit Jahren die steigende Verwendung von Scoringsystemen zur Diskriminierung von Bürgern. Der vorliegende Entwurf verpasst die Chance, die Scoringverfahren auf eine rechtliche Grundlage zu stellen. Notwendig ist eine Regelung, ähnlich dem deutschen Anpassungsgesetz, damit grundrechtswidrige Scoringverfahren endlich der Vergangenheit angehören.

Seit einigen Jahren macht die ARGE DATEN auf das zunehmende Problem der Verwendung von Scoringsystemen aufmerksam. Es handelt sich dabei um Systeme zur individuellen Beurteilung einer Person aufgrund allgemeiner oder statistischer Informationen und Erfahrungen. Im Rahmen dieser Scoringmethoden werden nicht für eine Sache unmittelbar erforderliche Informationen gesammelt und ausgewertet, sondern andere allgemeine erhebbare soziale, soziographische oder demoskopische Daten, die einer Person zugeordnet werden können. Im Gegensatz zu klassischen

[1] *Kühling/Martini et al.*, Die DSGVO und das nationale Recht, 2016 S 1 f.

Kreditbeurteilungssystemen, verwenden die neuen Scoringsysteme allgemeine Persönlichkeitsmerkmale zur Beurteilung der Betroffenen. So führt die arbeitsrechtliche Position einer Person als "Arbeiter" gegenüber einem Angestellten zu einem Bewertungsabschlag, ebenso wenn er ledig ist, wenn er in einer Mietwohnung ist, wenn er jung ist, wenn er erst kurz eine Arbeit hat oder auch wenn er schlicht in einer "falschen" Wohngegend wohnt. Damit werden im statistischen Sinn möglicherweise richtige Informationen auf individuelle Personen übertragen, unabhängig davon ob diese Person nicht durch ihr individuelles Verhalten eine völlig andere Beurteilung verdient. Damit wird die Variabilität der Informationen ignoriert, eine klassische sachlich unbegründete Ungleichbehandlung. Diese Scorings führen zum Ausschluss von bestimmten Leistungen, zu verschlechterten Kredit- und Versicherungskonditionen oder verhindern die Eröffnung eines Bankkontos.

Scorings enthalten somit ein erhebliches Diskriminierungspotential. Diese Scorings werden immer stärker von Telekom-Unternehmen, Versandhäusern, Banken, Leasingunternehmen und sogar von Vermietern, Möbelhändlern und Supporthotlines verwendet.

Die bisherigen Schutzmechanismen des DSG 2000, insbesondere § 49 DSG 2000, "Automatisierte Einzelentscheidungen" gegen die willkürliche Verwertung allgemeiner Persönlichkeitsangaben haben sich als nicht tragfähig erwiesen, da diese Regelungen auf eine vollautomatisierte Entscheidung abstellen, die jedoch beim Scoring in der Praxis nicht vorkommt. Die Scoringwerte werden offiziell nur als Empfehlungen ausgewiesen, wobei jedoch die Mitarbeiter (Verkäufer) der Unternehmen, die diese Scorings anwenden gar keine Möglichkeit haben eine andere Entscheidung zu treffen, als es das Scoring vorgibt. Auch die DSGVO regelt die Verwendung von Scoringsystemen unzureichend. Art. 22 DSGVO enthält dieselbe Regelungslücke wie § 49 DSG 2000. Der Betroffene hat bloß das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden.

Während in Deutschland eine Regelung dieser Scoringmethoden im Datenschutz-Anpassungs- und -Umsetzungsgesetz EU beschlossen wurde (siehe § 31 DSAnpUG-EU), fehlen im vorliegenden DSG 2018-Entwurf jegliche Ansätze zu Lösungsversuchen.

Es wird daher vorgeschlagen, die bestehenden Scoring-Exzesse so weit wie möglich zurückzudrängen und vorzusehen, dass Unternehmen, die Scoring einsetzen, diese Verfahren generell nach wissenschaftlich anerkannten mathematisch-statistischen ausführen müssen. Soweit Scoringverfahren Voraussetzung oder Grundlage eines Vertragsabschlusses darstellen, sollten die Verfahren den Interessenten vor Vertragsabschluss offengelegt werden müssen.

## 3. Datenschutz-Anpassungsgesetz 2018 macht Whistleblowing-Hotlines unzulässig

Die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten darf nach Art. 10 DSGVO nur unter behördlicher Aufsicht vorgenommen werden oder wenn dies nach dem Unionsrecht oder dem mitgliedsstaatlichen Recht zulässig ist.

Damit die Verarbeitung strafrechtlicher relevanter Daten zulässig ist, ist ein Erlaubnistatbestand erforderlich. Es reicht nicht aus, dass das DSG 2018 keine Bestimmung diesbezüglich enthält.

Die ARGE DATEN fordert den Gesetzgeber auf, klarzustellen, ob es die Intention ist, die Verarbeitung strafrechtlicher relevanter Daten nur unter behördlicher Aufsicht zuzulassen. Eine Klarstellung ist notwendig, da eine Vielzahl von Datenanwendungen wie z.B. Whistleblowing-Hotlines[2] von einer Regelung bzw. Nicht-Regelung betroffen sind.

## 4. § 1 – Grundrecht auf Datenschutz

Die Intention des Gesetzgebers, möglichst vielen Bestimmungen aus der alten Rechtslage auch unter dem Regime der DSGVO Geltung zu verschaffen, wird an dieser Stelle deutlich sichtbar. Die ARGE DATEN spricht sich aus zwei Gründen gegen die Beibehaltung des Grundrechts auf Datenschutz in § 1 des Entwurfs aus.

Zum einen ist das Grundrecht auf Datenschutz in Art. 8 Grundrechtecharta (GRC), der EMRK sowie der DSGVO umfassend und abschließend geregelt. Da der Schutzbereich des § 1 ohnehin von den genannten Bestimmungen überlagert wird, hat § 1 für die Grundrechtsträger keinen Mehrwert und führt lediglich zu einer Verkomplizierung der Rechtslage.

Zum anderen sind die in Abs. 2 aufgezählten Einschränkungstatbestände im nichthoheitlichen Bereich nicht deckungsgleich mit den in Art. 6 Abs. 1 DSGVO normierten Bedingungen für eine rechtmäßige Datenverarbeitung. Sohin scheint zumindest eine Anpassung der Einschränkungstatbestände des § 1 Abs. 2 DSG 2018 notwendig, um einen Konflikt mit der DSGVO zu verhindern. Alternativ könnte der Anwendungsbereich auch auf den hoheitlichen Bereich beschränkt werden.

## 5. § 3 – Durchführungsbestimmung

Auch in § 3 des Entwurfs zum DSG 2018 wird eine Regelung aus der alten Rechtslage übernommen (siehe § 27 Abs. 6 DSG 2000). Aus Sicht der ARGE DATEN ist § 3 nicht mit der DSGVO vereinbar. Die DSGVO sieht in Art. 17 vor, dass der Verantwortliche verpflichtet ist, Daten unverzüglich zu löschen. § 3 DSG 2018 macht davon eine Ausnahme, wenn die Löschung aus wirtschaftlichen oder technischen Gründen nur zu bestimmten Zeitpunkten vorgenommen werden kann. Bis zu dem Zeitpunkt ist die Verarbeitung einzuschränken.
Aus Sicht der Betroffenenrechte wäre eine Beschränkung des Rechts auf Löschung grundsätzlich über Art. 17 Abs. 3 lit a bis e DSGVO möglich. Aus dem Gesetzesentwurf geht jedoch nicht hervor, welches der in Art. 17 Abs. 3 lit a bis e aufgezählten Ziele erreicht werden soll. Wirtschaftliche oder technische Gründe sind jedenfals nicht ausreichend, sodass eine Beschränkung der Löschungsverpflichtung, wie in § 3 des Entwurfs vorgesehen, nicht mit der DSGVO vereinbar ist.

[2] Feiler/Forgo, EU-DSGVO, 2017, Art. 10 Rz. 1.

§ 3 DSG 2018 ist an die Zielvorgaben des Art. 17 Abs. 3 lit a bis e DSGVO anzupassen oder zur Gänze zu streichen.

## 6. § 5 Abs. 2 – Datenschutzbeauftragter im öffentlichen Bereich

§ 5 Abs. 2 des Entwurfs sieht als Besonderheit für die Bestellung eines Datenschutzbeauftragten im öffentlichen Bereich vor, dass dieser dem jeweiligen Bundesministerium oder der jeweiligen nachgeordneten Dienststelle oder sonstigen Einrichtung angehören muss.

Es ist nicht ersichtlich, auf welcher Grundlage diese Eingrenzung des Personenkreises für die Bestellung des Datenschutzbeauftragten vorgenommen wird. Aus Art. 37 Abs. 6 DSGVO ergibt sich vielmehr die Möglichkeit für Verantwortliche sowohl des öffentlichen als auch des nicht-öffentlichen Bereichs externe Datenschutzbeauftragte zu bestellen.
Ganz unabhängig, ob es sich bei einem Datenschutzbeauftragten um einen Beschäftigten des Unternehmens/der jeweiligen Diensstelle oder eine externe Person handelt, muss der Datenschutzbeauftragte seine „Pflichten und Aufgaben in vollständiger Unabhängigkeit ausüben […]“ (Erwägungsgrund 97). Der Verantwortlicher hat zu diesem Zweck sicherzustellen, dass der Datenschutzbeauftragte bei der Erfüllung seiner Aufgaben keine Anweisungen bezüglich der Ausübung seiner Aufgaben erhält (Art. 38 Abs. 3 DSGVO). In vielen Fällen wird die einzige Möglichkeit, die völlige Unabhängigkeit des Datenschutzbeauftragten im öffentlichen Bereich garantieren zu können, die Bestellung eines externen Datenschutzbeauftragten sein. In diesem Sinn steht § 5 Abs. 2 2. Satz in Konflikt mit der obligatorischen Unabhängigkeit des Datenschutzbeauftragten.

Der Passus „*Diese müssen dem jeweiligen Bundesministerium oder der jeweiligen nachgeordneten Dienststelle oder sonstigen Einrichtung angehören*“ sollte daher gestrichen werden.

## 7. § 11 – Befugnisse der Datenschutzbehörde

Gemäß § 11 DSG 2018 kann die Datenschutzbehörde nur im Fall eines „begründeten Verdachts“ auf Verletzung der in der DSGVO oder gegen das 1. oder 2. Hauptstück genannten Rechte und Pflichten, Datenverarbeitungen überprüfen. Die Bestimmung wurde fast wortgleich aus dem DSG 2000 übernommen (siehe § 30 Abs. 2 DSG 2000). Verkannt wird, dass die DSGVO die Untersuchungsbefugnisse der Aufsichtsbehörde in einem Mindestmaß in Art. 58 Abs. 1 festlegt. Über Art. 58 Abs. 6 DSGVO könnte der österreichische Gesetzgeber zusätzliche Befugnisse vorsehen, nicht jedoch Mindestbefugnisse der Datenschutzbehörde einschränken.

Die Einschränkung der Überprüfungsmöglichkeit von Datenverarbeitungen ist nicht mit Art. 58 Abs. 1 lit b DSGVO vereinbar, der als Untersuchungsbefugnis die Durchführung von Untersuchungen in Form von Datenschutzüberprüfungen vorsieht, unabhängig davon, ob ein „begründeter Verdacht“ vorliegt oder nicht.

## 8. § 13 Abs. 5 – Enscheidungen der Datenschutzbehörde gegenüber Verantwortlichen des öffentlichen Bereichs nicht durchsetzbar

Zum Bedauern der ARGE DATEN beweist der Gesetzgeber an dieser Stelle, wie wenig Interesse er an einem Datenschutz hat, der gleichermaßen für Unternehmen und öffentlich-rechtliche Einrichtungen gilt.
Aus einem Umkehrschluss aus § 13 Abs. 5 DSGVO ergibt sich: Gegenüber Verantwortlichen des öffentlichen Bereichs kann die Datenschutzbehörde Verletzungen der Bestimmungen der DSGVO und des DSG 2018 nur feststellen. Die Datenschutzbehörde hat gegen öffentlich-rechtliche Einrichtungen somit nicht die Möglichkeit Entscheidungen auch wirksam durchzusetzen.

Dass der Datenschutzbehörde die Durchsetzung ihrer Entscheidungen auch gegenüber Verantwortlichen im öffentlichen Bereich möglich sein muss, zeigen die zahlreichen (teilweise massiven) Verstöße der letzten Jahre. In zahllosen Verfahren wurden Datenschutzverletzungen von Behörden, Körperschaften und Ministerien festgestellt. Wenn sich jedoch die Behörde weigerte den datenschutzkonformen Zustand wieder herzustellen, dann gab es für die Bürger keine Durchsetzungsmöglichkeit.

Die Beschränkung der Durchsetzungsmöglichkeit von Entscheidungen der Datenschutzbehörde auf Verantwortliche aus dem privaten Bereich ist nicht nur aus Gründen des Rechtsschutzes äußerst bedenklich, sondern auch von der DSGVO nicht gedeckt. Nach Art. 58 Abs. 2 verfügt jede Aufsichtsbehörde über gewisse Abhilfebefugnisse, die es ihr gestatten, ihre Entscheidungen auch tatsächlich durchzusetzen. Die DSGVO trifft in diesem Zusammenhang keine Unterscheidung zwischen Verantwortlichen des öffentlichen Bereichs und Verantwortlichen des privaten Bereichs. Eine Einschränkung durch mitgliedstaatliche Gesetzgeber, wie in § 13 Abs. 5 des Entwurfs vorgesehen, ist somit mit der DSGVO nicht vereinbar.

Folglich hat § 13 Abs. 5 zu lauten:

*„(5) Soweit sich eine Beschwerde als berechtigt erweist, ist ihr Folge zu geben und die Rechtsverletzung festzustellen. Dem Verantwortlichen ist zusätzlich aufzutragen, den Anträgen des Beschwerdeführers auf Auskunft, Berichtigung, Löschung, Einschränkung oder Datenübertragung in jenem Umfang zu entsprechen, der erforderlich ist, um die festgestellte Rechtsverletzung zu beseitigen. Soweit sich die Beschwerde als nicht berechtigt erweist, ist sie abzuweisen.“*

Da der Anwendungsvorrang des Unionsrechts nicht nur gegenüber einfachgesetzlichem innerstaatlichen Recht sondern auch gegenüber dem Verfassungsrecht gilt, wären Bestimmungen der österreichischen Bundesverfassung anzupassen, falls dies notwendig ist um die Datenschutzbehörde mit den obligatorischen Abhilfebefugnissen gem. der DSGVO auszustatten.

## 9. § 17 – Vertretung von betroffenen Personen

Gemäß § 17 DSG 2018 kann ein Betroffener gewisse Einrichtungen, Organisationen oder Vereinigungen damit beauftragen das Recht auf Beschwerde, die Betroffenenrechte oder das Recht auf Schadenersatz, in ihrem Namen wahrzunehmen.

§ 17 des Entwurfs wiederholt insofern Art. 80 DSGVO, als Voraussetzung für die Vertretungsbefugnis der Einrichtung, Organisation oder Vereinigung u.a. ist, dass deren „satzungsmäßige Ziele im öffentlichen Interesse liegen". Völlig unklar ist allerdings, was das DSG 2018 in diesem Zusammenhang unter „öffentliches Interesse" versteht.
Die vorhandene Unklarheit geht auch zu Lasten der Betroffenen. Besteht im Zuge einer Schadenersatzklage, Zweifel am Vorliegen der Voraussetzungen der § 17 DSG 2018, hat die Datenschutzbehörde entsprechende Feststellungen mit Bescheid zu treffen, gegen den wiederum eine Beschwerde an das Bundesverwaltungsgericht möglich wäre (§ 11 Abs. 6 DSG 2018). Dadurch käme es zu einer sehr langen Verfahrensdauer bis überhaupt feststeht, ob die Einrichtung hinsichtlich der Schadenersatzklage vertretungsbefugt ist. Eine Definition, was in diesem Zusammenhang unter „öffentlichem Interesse" zu verstehen ist, ist daher auch für den wirksamen Betroffenenschutz unabdinglich.

Der Gesetzgeber sollte klarstellen, dass Einrichtungen, die sich der Durchsetzung der Grundrechte in Österreich verschrieben haben und dies in Ihren Satzungen festgelegt haben, jedenfalls als Einrichtungen gelten, deren „satzungsmäßige Ziele im öffentlichen Interesse liegen".

## 10. § 19 Abs. 1 und Abs. 2 – Allgemeine Bedingungen für die Verhängung von Geldbußen

Nach § 19 Abs. 1 des Entwurfs kann die Datenschutzbehörde Geldbußen gegen eine juristische Person nur verhängen, wenn eines ihrer Organe (in Führungsposition) einen Datenschutz-Verstoß entweder selbst begangen hat oder einen Verstoß durch einen Mitarbeiter (oder einer sonstigen für das Unternehmen tätigen Person) aufgrund mangelnder Kontrolle/Überwachung ermöglicht hat. Damit wird die Möglichkeit der Datenschutzbehörde zur Verhängung von Geldbußen gegen Unternehmen bei Fehlverhalten durch einen Mitarbeiter unzulässigerweise auf Fälle eingeschränkt, in denen auch ein Fehlverhalten eines Organs des Unternehmens nachweisbar ist.

Diese Regelungsweise entspricht nicht den Vorgaben der DSGVO, nach der ein Verstoß eines beliebigen Mitarbeiters zur Verhängung einer Geldbuße führen kann. § 19 DSG 2018 bedarf daher einer grundsätzlichen Überarbeitung.

## 11. § 19 Abs. 5 - Geldbußen gegen Behörden und öffentliche Stellen

Gegen Behörden und öffentliche Stellen können nach dem vorliegenden Entwurf keine Geldbußen verhängt werden. § 19 Abs. 5 DSG 2018 führt ähnlich wie § 13 Abs. 5 DSG 2018 dazu, dass die Effektivität der DSGVO massiv geschwächt wird. Im Ergebnis könnte die Datenschutzbehörde Behörden und öffentlichen Stellen weder Leistungsaufträge zur Herstellung des rechtmäßigen Zustands erteilen, noch abschreckende Maßnahmen in

Form von Geldbußen gegen diese verhängen. Diese Bestimmungen haben zur Folge, dass das Datenschutzrecht im öffentlichen Bereich zahnlos ist.

§ 19 Abs. 5 ist ersatzlos zu streichen und der Datenschutzbehörde muss die Entscheidung überlassen werden, auch gegen Behörden und öffentliche Stellen nach ihrem Ermessen wirksame, verhältnismäßige und abschreckende Geldbußen zu verhängen.

## 12. § 29 - Verarbeitung personenbezogener Daten im Beschäftigungskontext

In § 29 DSG 2018 wird auf das Arbeitsverfassungsgesetz (ArbVG) verwiesen, ohne konkreter auf die Konsequenzen im Falle des Verstoßes gegen Bestimmungen des ArbVG einzugehen. Damit bleibt die Frage offen, ob die Datenschutzbehörde bei einem Verstoß gegen die maßgeblichen Bestimmungen des ArbVG die Möglichkeit der Verhängung einer Geldbuße gemäß Art. 83 Abs. 1 DSGVO hätte. In diesem Zusammenhang wäre auf Grund der Höhe der möglichen Geldbuße eine klarstellende Bestimmung unbedingt notwendig.

## 13. § 30 Abs. 1 – Zulässigkeit der Bildaufnahme

Entgegen der Überschrift behandelt § 30 DSG 2018 nicht nur die Zulässigkeit von „reinen" Bildaufnahmen, sondern auch dabei mitverarbeitete akustische Informationen. Diese Regelungsweise, die den (falschen) Eindruck erweckt, dass Tonaufnahmen bis dato nicht unter das Datenschutzrecht gefallen sind und deren Zulässigkeit erst mit dem DSG 2018 „mitgeregelt" werden, ist systemwidrig und irreführend. Tatsache ist, dass Tonaufnahmen erhebliche Eingriffe in Persönlichkeitsrechte darstellen können und schon nach derzeitiger Rechtslage teilweise strengeren Regelungen unterliegen als Bildaufnahmen.[3]

Die Verarbeitung von akustischen Informationen ist nicht ins Regelungskonvolut der Bildaufnahme miteinzubeziehen. Sofern der Anwendungsbereich des Datenschutzrechts erfüllt ist, muss die Prüfung der Zulässigkeit einer Tonaufnahme in jedem Einzelfall – getrennt von der Zulässigkeitsprüfung der Bildaufnahme - anhand der datenschutzrechtlichen Grundsätze erfolgen.

Insofern ist der Satz *„Zur Bildaufnahme gehören auch dabei mitverarbeitete akustische Informationen"* zu streichen.

## 14. § 33 Abs. 2 - Ausnahmen von der Kennzeichnungspflicht

Die Ausnahme von der Kennzeichnungspflicht für Bildaufnahmen für „strikt zu begrenzende Verarbeitungen im Einzelfall, deren Zweck ausschließlich mittels einer

[3] So hat der Missbrauch von Tonaufnahme- oder Abhörgeräten unter Umständen strafrechtliche Konsequenzen. Nach § 120 Abs. 1 Strafgesetzbuch (StGB) ist mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bis zu 720 Tagessätzen zu bestrafen, wer ein Tonaufnahmegerät oder ein Abhörgerät benützt, um sich oder einem anderen Unbefugten von einer nicht öffentlichen und nicht zu seiner Kenntnisnahme bestimmten Äußerung eines anderen Kenntnis zu verschafft.

verdeckten Ermittlung erreicht werden kann“ ist äußerst problematisch. Zu befürchten ist, dass diese Bestimmung von vielen Betreibern von Videoüberwachungen extensiv interpretiert und zur Rechtfertigung von ausufender, verdeckter Ermittlungstätigkeit im privaten Bereich herangezogen wird.

Nicht praxisnah ist zudem die Bedingung, „dass der Verantwortliche ausreichende Garantien zur Wahrung der Betroffeneninteressen vorsieht, insbesondere durch eine nachträgliche Information der betroffenen Personen“. Bei einer verdeckten Videoüberwachung ist es in vielen Fällen unmöglich, alle erfassten Personen im Nachhinein zu informieren.

§ 33 Abs. 2 ist wie folgt, aufrechtzuerhalten: *„Die Kennzeichnungspflicht gilt nicht in den Fällen des § 30 Abs. 3 Z 3.“*