Votum Separatum DSG-Novelle 2008

von Dr. Hans G. Zeger zur Sitzung des Datenschutzrates vom 14. Juli 2008 betreffend ein Bundesgesetz, mit dem das Datenschutzgesetz 2000 geändert wird (DSG-Novelle 2008)

Inhalt

1. Einleitung

Mit dem Entwurf zur DSG-Novelle 2008 wurde es verabsäumt eine Reihe von Defiziten und Praxisproblemen im bestehenden Datenschutzrecht zu beheben.

2. Behebung der missglückten Konstruktion der Datenschutzkommission

Die europarechtswidrige Konstruktion der österreichischen Datenschutzkommission (DSK) ist seit Jahren einer der Hauptkritikpunkte am österreichischen Datenschutzrecht. Zwischen der europarechtlich garantierten „unabhängigen Kontrollstelle“ mit umfassenden Kompetenzen und der österreichischen Umsetzung einer „Rumpfbehörde“ liegen Welten. Nicht ohne Grund läuft deswegen ein EU-Vertragsverletzungsverfahren gegen die Republik Österreich. Durch eine Neuorganisation der Datenschutz-Aufsichtsstelle könnte dieses wenig schmeichelhafte Verfahren beendet werden.

Die grundsätzlichen Kritikpunkte, warum die DSK aus organisatorischen und formalrechtlichen Gründen nicht den Vorgaben der EU-Datenschutzrichtlinie entspricht, sind bekannt:

-) Der Datenschutzkommission fehlt eine verfassungsrechtliche Verankerungund und ist damit nicht einmal formal unabhängig.
-) Die organisatorische Eingliederung der Datenschutzkommission nebst Geschäftsstelle und Personal in die Behörde Bundeskanzleramt sowie die Stellung des "Bundesbeamten als geschäftsführendes Mitglied" sind mit Art. 22 der EU-Datenschutzrichtlinie unvereinbar.
-) Die DSK ist beim Bundeskanzleramt eingerichtet und hängt materiell vom Wohlwollen des Bundeskanzlers ab. Fehlende Budgethoheit, die fehlende Nachbesetzungsbefugnis, den fehlenden Einfluss auf Personal, nötigen die Datenschutzkommission zum Wohlverhalten gegenüber der Politik.
-) Die befristete Bestellung der Behördenmitgliedern ist dadurch, dass diese nach Ablauf ihrer Amtszeit wieder zur Behörde zurückkehren zu müssen, unvereinbar mit den Unabhängigkeitsgarantien.

Neben diesen organisatorischen und formalen Defiziten gibt es auch verfahrensrechtliche Komponenten, in denen die österreichische Datenschutzbehörde weit hinter den europäischen Rahmenregelungen zurück bleibt.

A. Fehlende wirksame Einwirkungsbefugnisse

Art. 28 der EU-Datenschutzrichtlinie garantiert hinsichtlich der nationalen Kontrollstelle wirksame Einwirkungsbefugnisse, darunter die Befugnis, die Sperrung, Löschung oder Vernichtung von Daten oder das vorläufige oder endgültige Verbot einer Verarbeitung anzuordnen.

In der österreichischen Gesetzesumsetzung liest sich derzeit die entsprechende Regelung ganz anders: Gemäß § 31 Abs 3 DSG 2000 kann die DSK im Zuge der Behandlung einer bereits eingebrachten Beschwerde bei Gefahr im Verzug die weitere Verwendung von Daten zur Gänze oder teilweise untersagen. Darüber hinaus gibt es nach § 20 Abs 2 DSG die Möglichkeit, bei Vorliegen einer wesentlichen Gefährdung schutzwürdiger Geheimhaltungsinteressen und Gefahr im Verzug während des Meldeverfahrens die Weiterführung der Datenanwendung mit Bescheid gemäß § 57 Abs 1 AVG vorläufig zu untersagen - der sogenannte Mandatsbescheid.

Die Möglichkeit der Untersagung ist zwar in das österreichische Gesetz eingeflossen, allerdings unter wesentlichen Einschränkungen: Mandatsbescheide können nur während des Meldeverfahrens erlassen werden und bedingen Gefahr in Verzug. Ist eine Datenanwendung gemeldet können Verbote der Verarbeitung durch die DSK nicht von sich aus - etwa im Rahmen einer amtswegigen Einschau - erlassen werden, sondern erst, sobald jemand Beschwerde erhoben hat.

In der Realität macht die DSK von dieser reduzierten Kompetenzen praktisch keinen Gebrauch: Ganze fünf Mandatsbescheide scheinen im RIS seit 2003 auf - zuletzt untersagte die DSK 2007 auf diesem Wege eine mehr als dubiose Pharmastudie. Bescheide gemäß §

31 Abs 3 DSG 2000 zeigt das RIS keine an, die DSK macht von dieser Kompetenz - aus welchen Gründen immer - keinen Gebrauch.

Von der offenkundigen Unwilligkeit der Behördenpraxis, gewährte Kompetenzen auch auszuüben, abgesehen, ist aber auch festzuhalten, dass die durch den österreichischen Gesetzgeber gewählten Einschränkungen in keiner Weise durch die europarechtlichen Vorgaben gedeckt sind. Weder finden sich in der EU-Datenschutzrichtlinie irgendwelche Erwägungen, dass die Möglichkeit der Sperrung, Löschung oder Vernichtung von Daten oder das vorläufige oder endgültige Verbot einer Verarbeitung nur im Meldeverfahren bzw. im Rahmen eines Beschwerdeverfahrens bzw. nur im Falle Gefahr im Verzugs bestehen soll. Die österreichische Regelung bleibt hier hinter den europarechtlichen Vorgaben zurück.

B. Mangelnde materielle Zuständigkeit

Das zweite Manko wird durch die Spruchpraxis der DSK selbst verursacht.

Wiederholt weist die Datenschutzkommission in Bescheiden darauf hin, dass sie nicht dafür zuständig wäre, mit Hilfe der Geltendmachung der Datenschutzrechte die Verfahrensführung anderer Behörden zu kontrollieren oder zu korrigieren. Nach Lesart der DSK sind datenschutzrechtliche Beschwerden nicht geeignet, in der Sache vor andere Behörden gehörende Rechtsfragen neuerlich prüfen zu lassen, da dies bewirken würde, dass die Datenschutzkommission – zumindest teilweise – an die Stelle der sachlich zuständigen Behörde tritt und sich im Umwege über den Abspruch über die Zulässigkeit von Sachverhaltsermittlungen eine sachliche Zuständigkeit anmaßen würde.

Beispiele, in denen die DSK ihre eigene Unzuständigkeit erklärt, sind die Entscheidung K121.005/0014/2007, wo sich die DSK de facto weigerte, über die datenschutzrechtliche Zulässigkeit einer Betriebsprüfung, bei der auch die Ehegattin eines Mitarbeiters unter dem Titel „Verdacht auf Steuerbetrug“ durchleuchtet wurde, abzusprechen oder die Entscheidung K 121.29/0006-DSK/2006, in welcher sich die DSK nicht zuständig sah, zu prüfen, welche Daten im Rahmen der Amtshilfe an eine andere Behörde, die Ermittlungsschritte in einem anhängigen Verwaltungsverfahren unternimmt, übermittelt werden dürfen.

In derartigen Fällen erfolgt durch die DSK nur eine formale Prüfung, ob - im Sinne der datenschutzrechtlichen Zulässigkeit - die Angemessenheit und Notwendigkeit entsprechender Datenverwendungen durch die betreffenden Behörden "denkmöglich" gewesen sei. Da alles "denkmöglich" sein kann gibt es im Endeffekt keine Überprüfung.

Konsequenz: Rechtmittel wegen Datenschutzverletzungen müssten bei den Sachbehörden (Finanzamt, Meldeamt, Gemeindeamt, ...) und nicht bei der datenschutzkommission eingebracht werden. Eine offensichtliche Verletzung der EU-Richtlinie, die vorgibt, dass für Datenschutzverletzungen eine unabhängige behörde zu schaffen und diese anzurufen ist.

In vielen Fällen könnte nicht einmal theoretisch die Sachbehörde angerufenw erden, da Datenschutzverletzungen auch dann stattfinden, wenn der Bürger gar nicht Verfahrenspartei ist und er erst von den Verletzungen erfährt, wenn die Verfahren längst abgeschlossen sind.

Ein weiteres Problem ist, dass selbst dann, wenn ein Rechtsmittel möglich ist, die Berufungsinstanzen in der Regel nicht aus weisungsfreien und unabhängigen Behörden bestehen.

Art. 28 der EU-Datenschutz-RL legt fest, dass die Mitgliedstaaten eine oder mehrere öffentliche Stellen beauftragen müssen, die Anwendung der von den Mitgliedstaaten zur Umsetzung dieser Richtlinie erlassenen einzelstaatlichen Vorschriften in ihrem Hoheitsgebiet zu überwachen. Diese Stellen haben die ihnen zugewiesenen Aufgaben in völliger Unabhängigkeit wahrzunehmen. Weiters ist gemäß Art. 22 der Richtlinie Betroffenen ein Rechtsmittel garantiert.

Die österreichische Situation, dass sich die DSK beharrlich weigert, verschiedene datenschutzrechtlich relevante Sachverhalte, die in die materiellrechtlichen Enzscheidungskompetenzen anderer Behörden fallen, zu prüfen, ist mit diesen Garantien unvereinbar. Eine partielle Überprüfungsmöglichkeit durch weisungsgebundene Behörden aus anderen Bereichen kann eine solche Garantie ebenso wenig ersetzen, wie die Möglichkeit höchstgerichtlicher Beschwerden, da in derartigen Verfahren keine Sachverhaltsermittlungen mehr durchgeführt und deren Überprüfungsmöglichkeit stark beschränkt ist.

C. Mangelnde Durchsetzungsbefugnisse im öffentlichen Bereich

Eine weitere Unvereinbarkeit mit der europarechtlichen Richtlinie betrifft die mangelnde Durchsetzbarkeit des in Art. 12 der Richtlinie 95/46/EG garantierten Auskunftsrechts gegenüber Auftraggebern öffentlichen Rechts nach der österreichischen Rechtsordnung.

Die Entscheidung K073.028/0004-DSK/2007 der DSK zeigt dieses Problem. Verletzungen des Auskunftsrechts durch das Bundesministerium für Finanzen, wurden gegenüber dem Betroffenen durch die DSK bereits in einer Vorgängerentscheidung K121.259/0013-DSK/2007 festgestellt. Da trotz Entscheidung der Datenschutzkommission dem Betroffenen entsprechende Auskunft nicht erteilt wurde, wurde bei der Datenschutzkommission als bescheiderlassender Behörde der Antrag gestellt, den wirksamen Bescheid gegen den Beschwerdegegner zu exekutieren.

Gegenüber Auftraggebern des öffentlichen Rechts sind allerdings Verletzungen der Bestimmungen des DSG 2000 nach § 40 Abs 4 des österreichischen DSG 2000 durch die Datenschutzkommission nur festzustellen, nicht jedoch deren Behebung durchzusetzen.

Aus Anlass eines Bescheides über die Verletzung des Auskunftsrechts ergibt sich eine Verpflichtung des Auftraggebers, den rechtskonformen Zustand herzustellen, exekutierbar sind derartige Bescheide gegen Auftraggeber des öffentlichen Rechts nach den österreichischen Bestimmungen nicht.

Diese Rechtsauffassung ist auch durch die Judikatur des österreichischen Verwaltungsgerichtshofs gedeckt, welcher bereits in 2005/06/0366 entschied, dass gegenüber Auftraggebern des öffentlichen Rechts im Falle von Verletzungen gegen das Datenschutzgesetz kein durchsetzbarer Leistungsauftrag erwirkt werden kann. Bei Entscheidungen handelt es sich um Feststellungsbescheide, welche nicht exekutierbar sind. Betroffene können nach österreichischer Rechtslage zwar Verletzungen

datenschutzrechtlicher Bestimmungen durch Auftraggeber öffentlichen Rechts feststellen lassen, durchsetzbar sind die Ansprüche nicht.

Art. 12 der Richtlinie 95/46/EG verankert das datenschutzrechtliche Auskunftsrecht. Art. 24 verpflichtet die Mitgliedstaaten dazu, geeignete Maßnahmen zu ergreifen, um die volle Anwendung der Bestimmungen der Richtlinie sicherzustellen und Sanktionen festzusetzen, die bei Verstößen gegen die zur Umsetzung der erlassenen Vorschriften anzuwenden sind. Entsprechend der Richtlinie 95/46/EG besteht nicht nur die Verpflichtung, gesetzliche Bestimmungen zu erlassen, sondern es ist für die Mitgliedsstaaten verpflichtend, mittels effizienter und geeigneter Regelungen für die Einhaltung der Bestimmungen zu sorgen.

Ein reiner Feststellungsbescheid, der nicht durchsetzbar ist reicht nicht aus. Da gegenüber Auftraggebern öffentlichen Rechts im österreichischen Recht die Möglichkeit einer effizienten Rechtsdurchsetzung - mangels Vollstreckbarkeit entsprechender Entscheidungen - nicht gegeben ist, ist die derzeitige Rechtslage mit den genannten Regelungen der Richtlinie 95/46/EG nicht vereinbar.

D. Zahnloses Auskunftsrecht

Eine weitere Unvereinbarkeit mit den europarechtlichen Rahmenbedingungen stellt die generell zahnlose Durchsetzungsmöglichkeit des Auskunftsrechts dar. Nach österreichischer Lesart des DSG kann zwar gegen Verletzungen des Auskunftsrechts eine Beschwerde an die DSK erhoben werden. Allerdings hat der Beschwerdegegner die Möglichkeit, einer Feststellung der Verletzung seiner Auskunftsverpflichtung durch nachträgliche Auskunftserteilung entgegen zu wirken. Egal wie unvollständig und rechtswidrig diese Auskunft ist. Die DSK weist immer die Beschwerden ab, der Bürger muss bei einer rechtswidrigen eine neue Beschwerde einbringen.

Bei einer Auskunftsfrist von 8 Wochen, weiteren acht Monaten des DSK-Bescherdeverfahrens, das überhaupt Auskunft erteilt wird und nochmals 8 Monaten beschwerdeverfahren wegen rechtswidriger Auskunft, weiters einer von der DSK per Bescheidfestgelegten Auskunftsfrist von 2-4 Wochen und einem daran anschließenden Exekutionsverfahren (nur bei privaten Datenverarbeitern) von weiteren 6-12 Monaten, führt das dazu, dass Bürger erst nach 18-30 Monaten (!!) erfahren, welche daten über sie gespeichert wurden. Ein Zeitraum, in dem üblicherweise Daten in vielen Branchen (Adressenverlage, Wirtschaftsauskunftsdienste, ...) längst gelöscht oder völlig unaktuell und längst geändert sind.

Als Beispiel für diesen gesetzgeberischen Missgriff soll die Entscheidung 2006/06/0330 des VwGH vom 27.9.2007 dienen, welche über die Beschwerde gegen einen Bescheid der DSK absprach, mit welchem sich die DSK geweigert hatte, eine Verletzung des Auskunftsrecht durch die GIS Gebühren-Info Service Gmbh festzustellen, da diese Auskunft im Zuge des eingeleiteten Beschwerdeverfahrens erteilt hatte.

Die Entscheidung des VwGH fiel - infolge langjähriger Vorjudikatur - wenig überraschend aus: Die Beschwerdegegnerin habe im Zuge des Verfahrens eine Auskunft erteilt, insoferne sei – ähnlich wie bei Löschungsbegehren - eine Verletzung des Auskunftsrechts nicht "im nachhinein" feststellbar.

§ 31 Abs 1 des DSG 2000, welcher die Beschwerdemöglichkeiten regle, sehe eine derartige Sanktion nicht vor. Im übrigen stelle die Tatsache, dass eine Auskunftsverletzung nicht im Rahmen eines Verfahrens feststellbar seien, auch keine Verletzung der EU-Datenschutzrichtlinie dar, so der VwGH, da ein derartiger Anspruch aus den dortigen Bestimmungen nicht ableitbar sei.

Diese österreichische Judikaturlinie, dass Verletzungen des Auskunftsrechts bei nachträglicher Auskunftserteilung nicht mehr verfahrensmäßig feststellbar sind, sind die österreichischen Bestimmungen - entgegen den höchstgerichtlichen Ausführungen - sehr wohl hinsichtlich ihrer europarechtlichen Vereinbarkeit fragwürdig.

Art. 8 der EU-Datenschutz-RL garantiert Betroffenen „frei und ungehindert in angemessenen Abständen ohne unzumutbare Verzögerung oder übermäßige Kosten" die Bestätigung, dass es Verarbeitungen sie betreffender Daten gibt oder nicht gibt, sowie Informationen über die Zweckbestimmungen dieser Verarbeitungen, die Kategorien der Daten, die Gegenstand der Verarbeitung sind, und die Empfänger oder Kategorien der Empfänger, an die die Daten übermittelt werden.

Eine Gesetzeslage, die es ungeahndet lässt, wenn Betroffene nur im Rahmen langwieriger Beschwerdeverfahren ihre Ansprüche gegenüber Datenverarbeitern durchsetzen können, ist mit dieser Auskunftsgarantie unvereinbar. Auftraggeber werden - mangels Sanktionen - heute geradezu eingeladen, Ersuchen erst im Rahmen eines Beschwrdeverfahrens zu beantworten. Die Gesetzeslage ist daher mit den Bestimmungen der Richtlinie 95/46/EG nicht vereinbar.

E. *Resumee*

Neben den bekannten organisatorischen Problemen zeigen sich auch eine Reihe kompetenzrechtlicher Defizite bei der Umsetzung der Datenschutzrichtlinie. Der Gesetzgeber und die Republik Österreich sind gefordert einen europarechtlich vertragskonformen Zustand herzustellen.

Dies umso mehr, als angeblich den Koalitionärsparteien Europa und die EU ein großes Anliegen ist, die Sicherung der Bürgerrechte fiel bisher nicht darunter.

3. Anpassung der Verwaltungsstrafsätze

Die bestehenden Verwaltungsstrafsätze sind seit Jahren nicht angepasst und für den gewerblichen Bereich geradezu lächerlich gering. Während der gewerbliche Datenverarbeiter, der vorsätzlich Daten (und ganze Datenbestände) entgegen den Bestimmungen des DSG übermittelt, selbst im Wiederholungsfall nur mit einer Maximalstrafe von 18.890 Euro rechnen muss (DSG §52 Abs.1), wird das Versenden eines einzigen Spammails mit einer Strafe von bis zu 37.000 Euro bestraft (TKG §109 Abs. 3).

Es wird daher angeregt die Höchststrafe auf das für gewerbliche Verwaltungsübertretungen übliche Strafausmaß von 50.000 Euro anzuheben und gleichzeitig, wie in vielen EU-Ländern üblich, eine Mindeststrafe einzuführen. Als Mindeststrafe wird der Betrag von 500 Euro für alle Delikte nach §52 DSG angeregt.

4. Behebung der Rechtsschutzlücken im Zusammenhang mit "indirekt personenbezogenen Daten

Das österreichische DSG geht von der Fiktion der "indirekt personenbezogenen Daten" aus. Diesen Begriff gibt es nach der EU-Richtlinie Datenschutz gar nicht, es handelt sich um ein österreichisches Kuriosum, welches - entgegen der europäischen Rahmenbedingungen - viele Datenarten von fundamentalen datenschutzrechtlichen Grundsätzen und Schutzmechanismen ausschließt.

Die EU-Richtlinie verwendet eine breite Definition von personenbezogenen Daten, unter die auch Daten fallen, die zwar ein Auftraggeber nicht ohne weiters einer Person zuordnen kann, wo dies aber mit Zusatzwissen, von welcher Stelle auch immer, möglich ist.

Derartige Daten gewinnen insbesondere im Zusammenhang mit Internet, Web2.0 und Onlinemarketing verstärkt an Bedeutung. Im Rahmen der Internetnutzung ist es üblich Benutzer durch Identifikatoren wie IP-Adressen, Cookies, Pseudonyme und Nic-Names zu identifizieren und verschiedenste Daten, inkl. sensibler Daten diesen Identifikatoren zuzuordnen. Auch wenn diesen Identifikatoren nicht unmittelbar eine formalrechtliche persönliche Identität (mit Name, Adresse, Geburtsdatum, Personaldokumentennummer, ...) zugeordnet ist, kann jederzeit, bei Vorliegen entsprechender rechtlicher Interessen, die Identität durch Zusatzinformationen ausgeforscht werden.

Diese Daten, IP-Adressen, Cookies, Pseudonyme und Nic-Names und die mit ihnen verknüpften Informationen sind nach EU-Recht völlig zu recht als bestimmbare personenbezogene Daten zu werten und unterliegen dem Schutz der EU-Richtlinie. Insbesondere hat der Betroffene auf Antrag die Möglichkeit seine subjektiven Datenschutzrechte, wie Auskunft, Information und Löschung wahrzunehmen.

In Österreich werden diese Rechte - offenkundig EU-widrig - generell unter Hinweis, dass es sich nur um "indirekt personenbezogenen Daten" handle, ausgeschlossen. Statt jedoch dieses Datenschutzproblem endlich in einer Novelle zu beseitigen, bleibt es unverändert bestehen.

Nach DSG 2000 ist die Verwendung von indirekt personenbezogenen Daten – auch sensibler Daten - ohne Einwilligung des Betroffenen zulässig.

Sensible Daten, welche die rassische und ethnische Herkunft von Personen, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder das Sexualleben betreffen dürfen nach geltender Gesetzeslage auch verwendet werden, wenn die betroffene Person dieser Verwendung nicht zugestimmt hat, sofern sie nur in indirekt personenbezogener Form vorliegen.

Das bedeutet beispielsweise, dass ohne Zustimmung der Betroffenen Datenanwendungen betrieben werden dürfen, die gesundheitliche Informationen über bestimmte Personen mit deren Sozialversicherungsnummer verknüpfen, solange die konkrete Person selbst für den Auftraggeber nicht identifiziert ist.

Die laut Datenschutzgesetz 2000 den Betroffenen einer Datenanwendung zugesicherten Rechte stehen in Bezug auf Anwendungen mit ausschließlich indirekt personenbezogenen Daten nicht zu. Dazu gehören das Recht auf inhaltliche Auskunft über eine Datenanwendung, das Recht auf Richtigstellung und Löschung bei unrichtigem Inhalt oder unzulässiger Datenverarbeitung sowie das Recht auf Widerspruch bei Verletzung schutzwürdiger Geheimhaltungsinteressen des Betroffenen.

Im Gegensatz dazu betont die Richtlinie, dass auch jene Daten personenbezogen sind, die einer Person „nur indirekt zugeordnet werden können". Bei der Frage, ob eine Person aufgrund bestimmter Daten ermittelbar ist, sollen nach den Erwägungsgründen der Richtlinie sämtliche Mittel berücksichtigt werden, die vernünftigerweise durch den Datenverarbeiter oder einen Dritten eingesetzt werden können, um die jeweilige Person zu ermitteln.

Keine Anwendung soll die Richtlinie nur auf Daten finden, die derart anonymisiert sind, dass sich die entsprechende Person überhaupt nicht mehr ermitteln lässt. Eine Unterscheidung danach, ob die Ermittlung einer Person aufgrund vorhandener Daten nur mit rechtswidrigen Mitteln möglich ist oder nicht, enthält die Datenschutzrichtlinie nicht.

Europarechtlich ist es somit nicht vereinbar, diese Gruppe von personenbezogenen Daten pauschal aus den wichtigsten Grundsätzen des Datenschutzes auszunehmen. Die österreichische Rechtslage widerspricht einmal mehr grundlegend dem Geist der europäischen Datenschutzrichtlinie.

In seiner Entscheidung zur „section-control" hat sich auch der VfGH klar gegen den Begriff des „indirekt personenbezogenen Datums" gestellt.

5. Fehlerhafte Bestimmungen bei der Anrufung der Zivilgerichte

§32 DSG regelt zwar die Anrufung der Zivilgerichte bei der Durchsetzung von Ansprüchen gegen Auftraggeber des privaten Bereichs, die Bestimmungen sind jedoch unklar, unvollständig und führen immer wieder zu Verfahrensverzögerungen und vermeidbaren Verfahrenskosten.

A. Unklare Zuständigkeiten

Mit dem bloß allgemeinen Verweis auf den Zivilrechtsweg (§32 Abs.1) ergeben sich insbesodnere in Wien Unklarheiten bezüglich der gerichtlichen Zuständigkeiten. Da es sich bei Auftraggebern im Regelfall um gwewerbliche Datenverarbeiter handelt, werden regelmäßig Klagen vor dem Wiener Landesgericht für Zivilrechtssachen zurückgewiesen und an das Handelsgericht Wien verweisen. Dies führt zu Verfahrensverzögerungen und zusätzlichen Kosten.

Hier wäre eine Novellierung dahingehend notwendig, als für Verfahren nach dem DSG jedes Zivilgericht zuständig ist in dessen Sprengel der Betroffene seinen gewöhnlichen Aufenthalt oder Sitz hat oder der Auftraggeber oder der Dienstleister seinen gewöhnlichen Aufenthalt.

B. Unzulässige Beschränkung der Durchsetzung einstweiliger Verfügungen

Klagen und Anträge auf Erlassung einer einstweiligen Verfügung nach dem DSG sind zwar bei jenem Landesgericht möglich, in dessen Sprengel der Betroffene seinen gewöhnlichen Aufenthalt oder Sitz hat, nicht jedoch bei jenem Landesgericht, in dessen Sprengel der Auftraggeber oder der Dienstleister seinen gewöhnlichen Aufenthalt.

Das bedeutet, das nur bei einem Teil der Rechtsdurchsetzung der Betroffenen die Wahlfreiheit bei der Anrufung des Gerichts hat. Einstweilige Verfügungen müssen immer bei jenem Landesgericht erfolgen, in dessen Sprengel der Betroffene seinen gewöhnlichen Aufenthalt oder Sitz hat

Es wird vorgeschlagen, diese sachlich nicht gerechtfertigte Differenzierung zu beseitigen und Klagen und Anträge auf Erlassung einer einstweiligen Verfügung bei beiden Gerichtsständen zu ermöglichen.

6. Beweisverwertungsverbot rechtswidrig gesammelter Daten

Grundsatz eines wirksamen Datenschutzes kann es nur sein, dass nur rechtmäßig ermittelte und verwendete Daten Rechtswirksamkeit entfalten dürfen. Aus diesen Gründen ist ein umfassendes Beweisverwertungsverbot für rechtswidrig ermittelte und verwendete Daten zu schaffen. Derartige Daten dürfen in Verwaltungs-, Zivil- oder Strafverfahren nicht verwendet werden.

Statt diesen Grundsatz im Datenschutzgesetz verstärkt zu verankern, erfolgt in der DSG Novelle eine Aufweichung. Durften bisher nach §8 Abs. 3 Z5 DSG Daten zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen nur dann verwendet werden, wenn die Daten rechtmäßig ermittelt wurden, fehlt nunmehr diese Einschränkung.

Damit wird ein völlig falsches Signal gesetzt. Die Bestimmung erweckt nunmehr den Eindruck, dass für die Rechtsdurchsetzung "jedes Mittel der Beschaffung von Daten recht ist". Die Streichung der Einschränkung wird abgelehnt.

Es wird daher eine Anpassung der entsprechenden Bestimmungen in Hinblick auf ein Beweisverwertungsverbot rechtswidrig ermittelter und verwendeter Daten angeregt.

7. Missglückter Regelungsversuch Videoüberwachung

Ziel allgemeiner Datenschutzbestimmungen kann es niemals sein, in einem Datenschutzgesetz Ermächtigungen zum Einsatz von Datenverarbeitungen zu definieren. Dies muss Materiegesetzen vorbehalten bleiben.

A. Gescheiterter Videoüberwachungs-Entwurf

§50a des Entwurfes sieht in Abs. 3 eine Überfülle von Ermächtigungen vor, in denen Videoüberwachung keine "schutzwürdigen Geheimhaltungsinteressen" verletzt und somit generell zulässig ist. Die Bestimmungen im Einzelnen sind in sich widersprüchlich und unklar und letztlich entbehrlich, hält doch Z7 abschließend fest, dass jede "Videoüberwachung zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche des Auftraggebers vor einem Gericht" zulässig sei. Da Vandalismus, Besitzstörung, Einbrüche, aber auch Kündigungen eines Mieters oder Entlassung eines Mitarbeiters gerichtsanhängig werden können, wird damit ein Freibrief für jede Videoüberwachung geschaffen.

Mit der neuen Bestimmung ist die Videoüberwachung durch Private praktisch überall und an allen Orten möglich. Während die Rechtssprechung bisher davon ausging, dass Videoüberwachung nur zur Lösung bestimmter, meist strafrechtlicher Konfliktsituationen einzusetzen ist (etwa Aufklärung und Verhinderung von Einbrüchen, Überfällen oder Diebstählen), fällt diese Beschränkung im neuen Entwurf weg.

Jedes öffentliche Verhalten, soll in Zukunft, ohne jede andere Voraussetzung überwacht werden dürfen (§50a Abs.3 Z2).

Die Hauszufahrt des Nachbarn, der Schanigarten des Konkurrenten, jede Kamera in Fußgängerzonen, selbst Kameras in Diskotheken oder Cafes, in Bussen, U-Bahnen oder Eisenbahnzügen wären nach dieser Bestimmung völlig voraussetzungsfrei zulässig. Der Entwurf bleibt damit hinter der bisherigen Rechtssprechung des OGH zurück, der unter anderem eine Videoüberwachung öffentlichen Verhaltens (Betreten und Verlassen eines Hauses) als unzulässig angesehen hat.

Bedeutsam ist auch, dass nach dieser Bestimmung jede Videoüberwachung des Straßenverkehrs, unabhängig von Gefahren- oder Gefährdungssituationen zulässig wäre, inklusive einer flächendeckenden Überwachung durch die Asfinag, die schon seit Jahren auf deren Wunschzettel steht.

Eine weitere Vollmacht zu unbeschränkter Überwachung besteht in der willkürlichen Festlegung der 100.000,- Euro Wertgrenze (§50a Abs 3 Z5 lit. d). Was auf den ersten Blick nach viel aussieht, entpuppt sich als weitere Generalermächtigung. Es wird wohl keinen Betrieb und kein Geschäftslokal geben, in dem nicht die Waren und Geschäftsunterlagen diesen Wert übersteigen werden. Selbst die meisten Wohnungen haben mittlerweile einen darüber liegenden Einrichtungswert. Gleichzeitig ist die Grenze völlig willkürlich und unsinnig gezogen, könnte doch der Verlust eines kleineren Betrages eines weniger begüterten Menschen existenzbedrohender sein, als 100.000,- bei jemandem, der schon mal diesen Betrag im Casino verspielt.

Tatsächlich ist jedenfalls der gesamte Absatz 3 des Videoparagraphen § 50a entbehrlich. Die Voraussetzungen für eine Datenverarbeitung sind im DSG längst unter §6 DSG allgemein umschrieben. Jede weitere "Präzisierung" hätte nur die Konsequenz, dass zusätzliche Datenverarbeitungen erlaubt wären.

Es wird daher empfohlen den §50a Abs. 3 ersatzlos zu streichen, die für eine Videoüberwachung erforderlichen Voraussetzungen müssen in den Materiegesetzen geregelt werden nd sind nach den Anforderungen des §6 DSG zu prüfen.

Bisher ist die Rechtssprechung davon ausgegangen, dass Aufzeichnungen, die für einen Zweck, z.B. Diebstahlsüberwachung eines Verkaufsraumes, angefertigt wurden, nicht für einen anderen Zweck verwendet werden durften. Selbstverständlich war die Verwendung des Materials für die Anzeige des Diebstahls zulässig, selbstverständlich konnte das Material auf Grund eines Gerichtsbeschlusses auch in anderen Gerichtsverfahren vorgelegt werden.

B. Kein ausreichender Schutz höchstpersönlicher Lebensbereiche

Nicht einmal die Überwachung in höchstpersönlichen Lebensbereichen wird ausreichend verhindert. Diese Bereiche werden nicht ausreichend umschrieben, die erläuternden Bemerkungen beschränken sich auf Privatwohnungen, Toilettenanlagen und Umkleidekabinen. Private Verrichtungen finden aber auch an einer Vielzahl weiterer Stellen statt, zu denken ist an die Andacht am Friedhof oder in der Kirche, an Krankenzimmer oder Gymnastikräume, aber auch Hotelzimmer.

Der Entwurf fällt sogar hinter eine Reihe von OGH-Entscheidungen zurück, in denen der Bereich vor einer Privatwohnung oder der eigene Garten als höchstpersönlicher Lebensbereich definiert ist. Tritt der Entwurf in Kraft, müsste wieder in jahrelangen Verfahren ausgelotet werden, was unter "höchstpersönlichem Lebensbereich" gemeint ist. Es ist dem Gesetzgeber zuzumuten, dass dieser Punkt eindeutig im Gesetz definiert wird.

Die Mindestforderung ist, dass im Gesetz jene höchstpersönlichen Lebensbereiche definiert sind, in denen Videoüberwachungen verboten bzw. nur unter den Bedingungen des Großen Lauschangriffs erlaubt sind.

C. Sachlich unbegründete Differenzierungen verschiedener Überwachungsmethoden

Pauschal werden Echtzeitüberwachungen und Aufzeichnungen auf einem "analogen" Speichermedium von der Registrierungspflicht ausgenommen (§50c Abs.1 Z1,2).

Dies ist sachlich unbegündet. Ein Eingriff in die Privatsphäre findet etwa auch dann statt, wenn, wie schon 2007 VfGH-Präsident Korinek kritisierte, jemandem bei der Trauer am Friedhof zugeschaut wird. Echtzeitüberwachungen können unter Umständen sogar schwerwiegendere Eingriffe darstellen, als eine Aufzeichnung, die unter Verschluss ist, die niemand ansieht und die nur bei einem Strafdelikt für den bestimmten Zeitraum geöffnet wird.

Die Vorstellung ist unerträglich, aber durch den Gesetzesentwurf abgesegnet, dass wurstsemmelkauende, witzereißende Schulabbrecher als sogenanntes Sicherheitspersonal den Menschen bei ihrer Andacht zusehen.

Besonders ärgerlich ist die Ausnahme der "analogen" Speichermedien. Die EU-Richtlinie "Datenschutz" schreibt völlig eindeutig Schutzmaßnahmen vor, sobald Personen bestimmt oder bestimmbar sind (Art. 2 lit a 95/46/EG). Selbstverständlich sind auch Personen auf

Aufnahmen auf einer VHS-Kasette bestimmbar. Diese Ausnahmebestimmung ist eindeutig EU-widrig.

D. Lösung des Videoüberwachungsproblems

Der grundsätzliche Mangel des Entwurfs ist, dass er sich nicht mit der Frage auseinander gesetzt hat, was eigentlich eine Videoüberwachung von anderen Datenverarbeitungen unterscheidet. Nur diese Unterschiede rechtfertigen, dass es Sonderregeln für die Videoüberwachung gibt.

Kern des Unterschieds ist, dass bei allen Datenschutzregeln davon ausgegangen wird, dass eine Datenanwendung zu einem bestimmten Zweck eingerichtet ist (§4 Z7 DSG) und nur Daten von Personen enthält, die diesem Zweck entsprechen (§6 DSG).

Eine Mitarbeiterdatenbank darf nur Mitarbeiter enthalten, alle anderen sind zu löschen, eine Kundendatenbank nur Kunden usw.

Diese doppelte Zweckbestimmng, einerseits die Datenanwendung selbst unterliegt einem berechtigten Zweck, andererseits jeder Datensatz erfüllt diesen Zweck, ist bei der Videoüberwachung nicht gegeben.

Viele Videoüberwachungen erfüllen selbst keinen berechtigten Zweck im Sinne des §4 Z7, ihre Installationen sind bloß Ausdruck einer diffusen Angst, "dass etwas passieren könnte".

Selbst wenn jedoch die Vorbedingung einer klaren Zweckbestimmung der Installation erfüllt ist, ist für die Mehrzahl der ermittelten Daten nicht §6 DSG erfüllt. Es liegt in der Natur einer Videoüberwachung, die zum Beispiel gegen Ladendiebe installiert ist ("Zweck der Datenanwendung"), dass sie mehrheitlich Personen filmt, die nicht in den Anwendungsbereich fallen, schlicht keine Ladendiebe sind.

Es werden somit massenhaft Daten aufgezeichnet, die für den Zweck der Datenanwendung nicht wesentlich sind (§6 Abs. 1 Z3). Derartige Daten dürfen aber nicht aufbewahrt werden (§6 Abs.1 Z4,5) und sind unverzüglich zu löschen (§27 Abs.1 Z1).

Wir haben daher bei Videoüberwachungen das grundsätzliche Problem, dass einerseits Daten aufgezeichnet werden, die man gar nicht aufzeichnen dürfte (vereinfacht gesagt alle "Nicht-Täter") und zweitens, wenn sie schon aufgezeichnet sind, dass sie ehebaldigst zu löschen wären.

Eine sinnvolle Video-Datenschutzbestimmung muss sich daher auf genau diese Punkte beziehen, die abweichend von anderen Datenanwendungen sind.

Das Problem der Aufzeichnung von "Nicht-Tätern" kann durch Installation und Art und Weise des Betriebs reduziert werden. Eine Anlage, die nur einen Kassenraum überwacht wird weniger "Nicht-Täter" filmen, als eine die auch gleich den ganzen Vorplatz eines Geschäfts überwacht.

Kameras, die Überfälle dokumentieren sollen, werden kürzere Speicherfristen haben, als solche, die komplexe Betrügereien dokumentieren sollen. Es ist einem Geschäftsinhaber zuzumuten, am Ende eines Tages zu wissen, ob er überfallen wurde oder nicht.

Kern der Video-Datenschutzbestimmung muss daher das Zulassungsverfahren sein. Dieses ist jedoch im vorliegenden Entwurf völlig unzureichend geregelt.

Es muss gefordert werden, dass zu jeder Videoinstallation ein ausreichender Zweck genannt wird, dass detaillierte Installationspläne vorgelegt werden, die die Registrierungsbehörde in die Lage versetzen, zu erkennen welche Personen von der Überwachung erfasst sind. Weiters sind detaillierte Zugriffs- und Löschpläne vorzulegen, nach denen der Zugriff auf die Daten der "Nicht-Täter" beschränkt wird und eine ehebaldige Löschung sicher gestellt wird.

Die Zulassungsbehörde muss auch verpflichtet werden, vergleichbar jeder anderen Bau- oder Anlagengenehmigungsbehörde die Zweckmäßigkeit - in Hinblick auf die minimale Erfassung der "Nicht-Täter" - der Anlage vor Ort zu prüfen und gegebenenfalls Verbesserungen aufzutragen.

Die Vorschläge dazu sind im vorliegenden Entwurf völlig unzureichend.

Weiters sind umfassende Informationspflichten vorzusehen. Auch die Information über die Videoüberwachung ist im Entwurf nicht EU-konform umgesetzt. §50d erlaubt das Entfallen der Kennzeichnung und der Information der Betroffenen, bei "Unwahrscheinlichkeit der Beeinträchtigung der Betroffenenrechte", eine Formulierung, die eindeutig EU-widrig ist.

Die EU-Richtlinie sieht in Art. 10 und 11 eine generelle Informationpflicht vor, die nicht durch Klauseln beschränkt werden darf.

Auf Grund der Besonderheiten von Videoüberwachungen sind jedenfalls Informations- und Auskunftsrechte vorzusehen, die es Betroffenen erlauben, zu erkennen wo und mit welchen Wirkungskreis Videoinstallationen vorhanden sind. Dies könnte durch eine Erweiterung der Auskunftspflichten aus dem Datenverarbeitungsregister geschehen.

Schutz- oder Geheimhaltungszwecke können dieser erweiterten Informationspflicht nicht entgegenstehen, da Videoüebrwachung vorrangig präventiven Charakter hat und daher das Wissen, wo Installationen bestehen, diese präventive Aufgabe noch unterstützen. Ausnahmen von einer derartigen umfassenden Informationspflicht könnte bestenfalls bei Installationen erfolgen, deren ausschließlicher Zweck das Auffinden eines konkret Tatverdächtigen ist.

Auf Grund der besonderen Gefährdung der Datenschutzinteressen der Gruppe der "Nicht-Täter", die die Mehrzahl darstellt, sind auch die Auskunftsrechte auf diese spezifischen Bedürfnisse abzustellen.

Da ein "Nicht-Täter" von Videoinstallationen wiederholt gefilmt werden kann, etwa bei jedem Einkauf oder bei jedem Zutritt zu einem Haus, obwohl es keinerlei Verdachtsmomente oder Hinweise gibt, er könnte ein "Täter" sein, müssen auch die Auskunftsrechte besondere Garantien enthalten.

Ein einmaliges kostenloses Auskunftsrecht pro Jahr ist nicht ausreichend, da ja auch die Aufzeichnungen mehrfach erfolgen, aber bei den "Nicht-Tätern" keinesfalls so lange aufbewahrt werden dürfen. Der Auskunftsanspruch muss sich daher aus jeder neuerlichen Erfassung ergeben.

Auch eine Anpassung der Auskunfts- und Löschungsfristen ist erforderlich. Auf Grund der kurzen Aufbewahrungsdauer hat ein Auskunftsbegehren von Videoaufzeichnungen jedenfalls die Löschung der Daten zu hemmen. Um das Auskunftsrecht sinnvoll in Anspruch nehmen zu können ist auch erforderlich, dass die Aufbewahrungsfrist der Videoaufzeichnungen Teil der Informationspflicht wird.

Auf diese spezifischen Videoanforderungen nimmt der Entwurf keine Rücksicht.

Die Beschränkung der Auskunft auf eine Art Nacherzählung, was auf dem Video aufgezeichnet ist (§50e), widerspricht dem EU-Auskunftsrecht und ist abzulehnen.