RA Dr. Clemens Thiele, LL.M. Tax (GGU)

Aktuelles zur Videoüberwachung: Novelle zur StMV 2004

Am 30. 3. 2011 wurde die Novelle zur StMV 2004 kundgemacht,[1] die neben einigen (bloß) sprachlichen Änderungen auch eine Neufassung der SA013 („Personalverwaltung des Bundes und der bundesnahen Rechtsträger") sowie der SA015 („Personalverwaltung der Länder, Gemeinden und Gemeindeverbände") enthält. Darüber hinaus hat sie die aus dem Jahr 2010 stammende SA032 „Videoüberwachung" um einen Abschnitt F. erweitert, der die Voraussetzungen der zulässigen Videoüberwachung für „Ausländische Vertretungsbehörden und Internationale Organisationen" näher regelt. Der folgende Beitrag nimmt eine Einschätzung vor und versucht erste Begriffsklärungen.

1. Meldepflicht

Grundsätzlich unterliegen alle Videoüberwachungen durch Private der Meldepflicht und der Vorabkontrolle nach § 17 Abs 1 iVm § 19 DSG. Dies bedeutet, dass eine private Videoüberwachung im Grundsatz erst dann vorgenommen werden darf, wenn die entsprechende technische Anlage von der Datenschutzkommission genehmigt und ggf unter Erteilung von Auflagen bescheidmäßig erlaubt worden ist.

Eine entsprechende Antragstellung *vor* Inbetriebnahme der Anlage,[2] in der sowohl das technische System als auch der genaue Standort und die Art der Videoüberwachung dargelegt werden müssen, ist erforderlich, sofern nicht eine „nicht meldepflichtige Datenanwendung" nach § 17 Abs 2 DSG vorliegt. Die Meldung an die DSK erfolgt zum Zweck der Registrierung im DVR und dient der Publizität der Datenanwendung, insb der Gewährleistung des jedermann zustehenden Einsichtsrechts nach § 16 Abs 2 DSG.

2. Geänderte Standard- und Musterverordnung

§ 17 Abs 2 Z 6 DSG nimmt sog „Standard- oder Musteranwendungen" von der allgemeinen Vorabmeldepflicht des Auftraggebers aus. Dabei handelt es sich um durch Verordnung des Bundeskanzlers[3] festgelegte Typen von Datenanwendungen, die massenhaft in gleichartiger Weise vorgenommen werden, wie zB Rechnungswesen, Personalverwaltung für privatrechtliche Dienstverhältnisse, Mitgliederverwaltung, Kundenbetreuung und Marketing für eigene Zwecke oder Patientenverwaltung und Honorarabrechnungen für Ärzte.

Die Novelle 2011 zur Standardanwendung „SA032 Videoüberwachung" nimmt seit ihrem Inkrafttreten am 31. 3. 2011 zusätzlich auch Videoüberwachungen für ausländische Vertretungen und Internationale Organisationen von der Meldepflicht beim Datenverarbeitungsregister aus. Demzufolge handelt es sich um eine Erweiterung der „geschäftsbezogenen" oder „geschäftlichen" Videoüberwachung im „beschränkt öffentlichen Raum"[4] Die Ausnahme von der Meldepflicht reicht lediglich soweit, als dies zur Verwirklichung des Zwecks der Datenanwendung notwendig ist.

3. Voraussetzungen des Abschnitts F.

3.1. Besondere Zweckgebundenheit und überwachte Räume

Zunächst betrifft Abschnitt F. nur eine verschlüsselte Videoüberwachung zum Zweck

- des Eigentumsschutzes und
- des Verantwortungsschutzes (Wahrnehmung von Verkehrssicherungspflichten, Vertragshaftung gegenüber Benutzern etc) sowie
- zur Verhinderung, Eindämmung und Aufklärung strafrechtlich relevanten Verhaltens, insoweit davon der Aufgabenbereich des Auftraggebers betroffen ist,

mit ausschließlicher Auswertung in dem durch den Zweck definierten Anlassfall. Aus dem Rechtsverweis auf das „Wiener Übereinkommen über diplomatische Beziehungen" (WDK)[5] bestimmt sich die *„ausländische Vertretungsbehörde"* zunächst für die Auftraggebereigenschaft als Vertretungsbehörde eines fremden, dh nicht-österreichischen, Staates. Es muss sich dabei um Vertreter von ausländischen Staaten handeln, zu denen Österreich diplomatische Beziehungen unterhält bzw die Mitglieder des WDK sind.[6] In Betracht kommen diplomatische Missionen, berufskonsularische Vertretungen sowie ständige Vertretungen bei internationalen Organisationen, die ihren Amtssitz in Österreich haben.[7] Der Begriff der *„Internationalen Organisation"* umfasst nach völkerrechtlichem Verständnis[8] alle zwischenstaatlichen oder öffentlichen Internationalen Organisationen, die idR auf einem völkerrechtlichen Vertrag beruhen und ein Minimum an institutionalisierten Einrichtungen, insb Organe, und eine gewisse Dauerhaftigkeit besitzen. In Betracht kommen zB die Vereinten Nationen (und deren Teilorganisationen), die Europäische Union, die NATO, die OECD oder der Europarat; nicht hingegen zB Amnesty International oder Greenpeace, da diese Internationalen Non-Governmental Organisationen (INGO) nicht auf völkerrechtlichem Vertrag beruhen.[9]

In räumlicher Hinsicht erfasst die nicht meldepflichtige[10] Videoüberwachung den „Eingang" und den „Zutrittsbereich" sowie die „Fassade" von ausländischen Vertretungsbehörden und Internationalen Organisationen. Die zugehörige – einer Videoüberwachung zugängliche

1) BGBl II 105/2011.
2) Vgl § 18 DSG.
3) Standard- und Muster-Verordnung 2004 (StMV 2004), BGBl II 312/2004 idF BGBl II 255/2009, BGBl II 152/2010 und BGBl II 105/2011.
4) Vgl zur begrifflichen Unterscheidung *Thiele*, Aktuelles zur Videoüberwachung – Erste Erfahrungen nach der DSG Novelle 2010, jusIT 2010, 219, 220 rSp, gemäß dem Anhang zum Datenschutzbericht 2005-2007, 64 ff, abrufbar unter http://www.dsk.gv.at/DocView.axd?CobId=30637 (4. 4. 2011).
5) BGBl 66/1966 (StF).
6) Vgl die alphabetisch geordnete Aufzählung der Staaten am Beginn des WDK (183 Unterzeichnerstaaten; Stand 16. 5. 2011).
7) Vgl Art 3 Abs 1, 14 iVm Art 36 WDK.
8) Vgl *Neuhold/Hummer/Schreuer*, Österreichisches Handbuch des Völkerrechts I² (1991) Rz 811 ff mwN.
9) Vgl *Neuhold/Hummer/Schreuer*, Handbuch I² Rz 1107.
10) Jedoch müssen die genannten Auftraggeber nach § 23 DSG auf Anfrage mitteilen, welche Standardanwendungen sie tatsächlich vornehmen.

– feste Einrichtung kann mE nach Art 1 lit i WDK am besten mit dem Ausdruck „Räumlichkeiten der Mission" definiert werden, und bezeichnet demzufolge ungeachtet der Eigentumsverhältnisse die Gebäude oder Gebäudeteile und das dazugehörige Gelände, die für die Zwecke der Mission verwendet werden, einschließlich der Residenz des Missionschefs.[11] Die von der Videoüberwachung erfassten Außenteile der Mission ergeben sich aus dem allgemeinen Wortverständnis für den

- *„Eingang"*: Tür, Öffnung durch die man hineingehen, ein Gebäude, einen Raum, ein umgrenztes Gelände betreten kann;[12]
- *„Zutrittsbereich"*: dem Hineingehen, Eintreten oder Betreten dienende Flächen;[13] oder die
- *„Fassade"*: vordere (gewöhnlich der Straße zugekehrte) Außenseite eines Gebäudes; Front; Vorderseite.[14]

Die Kamerastandorte müssen also so gewählt sein, dass lediglich Außenanlagen des Missionsgebäudes erfasst werden, die iwS eine Zutrittskontrollfunktion erfüllen.

3.2. Erfasste Daten der Videoüberwachung

Als zu verarbeitende Datenarten (samt Historie) kommen in allen Fällen neben dem Ort[15] und der Zeit[16] der Bildaufzeichnung zunächst die Bilddaten[17] der Betroffenen, die sich im überwachten Bereich aufhalten, in Betracht (allgemeine Überwachungsdaten).

Darüber hinaus dürfen die Bilddaten[18] von Personen aufgezeichnet werden, die im Rahmen der Videoüberwachung aufgenommen und im Anlassfall identifiziert werden (anlassfallbezogene Bilddaten). Von diesen Personen dürfen in weiterer Folge sowohl deren Identität[19] als auch deren Rolle (zB Täter, Opfer, Zeuge) aufgezeichnet werden, soweit Letztere aus der Aufzeichnung erkennbar sind.

11) *„Missionschef"* ist nach Art 1 lit a WDK jene Person, die vom Entsendestaat beauftragt ist, in dieser Eigenschaft tätig zu sein, maW der leitende Diplomat, Botschafter oder Konsul.
12) *Duden*, Deutsches Universalwörterbuch, 318 rSp.
13) Vgl *Duden*, Deutsches Universalwörterbuch, 1497 mSp.
14) *Duden*, Deutsches Universalwörterbuch, 393 rSp.
15) Räumlichkeit, Standort der Kamera.
16) Datum, Uhrzeit, Beginn/Ende der Bildaufzeichnung.
17) Aussehen, Verhalten.
18) Aussehen, Verhalten.
19) Soweit aus der Aufzeichnung für den Auswertenden erkennbar.

3.3. Protokollierungspflicht

Für die Überwachung des (beschränkt) öffentlichen Raumes im Bereich von Missionsgebäuden nach Abschnitt F. besteht gem § 50b Abs 1 DSG eine Protokollierungspflicht des Auftraggebers für jeden Verwendungsvorgang. Daraus müssen die Betriebszeiten bzw Aufzeichnungszeiten und Speicherungen ersichtlich sein. Außer im Fall der Echtzeitüberwachung ist jeder Verwendungsvorgang von Bilddaten, dh der allgemeine und der anlassbezogene, „lückenlos zu protokollieren".[20] Die Verpflichtung zur Protokollierung umfasst mE demnach nicht nur die Aufzeichnung der überwachten Ereignisse selbst, sondern auch die Zugriffe und Auswertungen,[21] dh

- die Einrichtung und die per Einstellung aktivierten Funktionen der Anlage zu dokumentieren;
- die Betriebstätigkeit an den Anlagesystemen in einem Logbuch festzuhalten;
- den Zugriff auf gespeicherte Daten zu Auswertungszwecken oder zur Überprüfung der Funktionsfähigkeit zu dokumentieren;
- Zugriffe auf Bilddaten unter Angabe der Person und des Anlasses in geeigneter, dh nachvollziehbarer und dauerhafter Form festzuhalten;
- alle Auswertungen in einem Protokoll festzuhalten, aus dem hervorgeht, wer wann aus welchem Anlass und auf welche Speichermedien zugegriffen hat.

Die jeweilige Nutzung ist schriftlich zu fixieren. Aus dem Aspekt der Datensicherheit folgt, dass der Auftraggeber sicherzustellen hat, dass die aufgezeichneten (Bild-)Daten nicht verändert werden können. Der Zugriff muss beschränkt werden. Einem Teil der Lehre[22] ist demnach darin beizupflichten, dass der Betreiber zweckmäßigerweise eine Videoüberwachungsordnung zu erstellen hat.

3.4. Höchstdauer der zulässigen Datenaufbewahrung

Die Videodaten sind in allen Fällen spätestens nach 72 Stunden zu löschen; es gilt die Regel des § 50b Abs 2 Satz 2 DSG, wonach § 33 Abs 2 AVG auf die Fristberechnung anzuwenden ist. Fällt demnach das Ende der Aufbewahrungsfrist auf einen Samstag, Sonntag, gesetzlichen Feiertag oder den Karfreitag, so ist der nächste Werktag letzter Tag der Frist.

20) EBRV 485 BlgNR 24. GP, abgedruckt in der Textausgabe *ProLibris*, DSG[3] (2010), 198 f; *Pollirer/Weiss/Knyrim*, DSG § 50b Anm 1.
21) Arg: *„..., soweit aus der Aufzeichnung für den Auswertenden erkennbar"*.
22) *Pollirer/Weiss/Knyrim*, DSG § 50b Anm 1.

3.5. Zulässige Empfängerkreise

Die durch eine Videoüberwachung gewonnenen Daten dürfen ausschließlich im Anlassfall von den Auftraggebern des Abschnitts F. an die Sicherheitsbehörden und die Staatsanwaltschaft zu Zwecken der Beweismittellieferung in Strafrechtsangelegenheiten weitergegeben werden. An die Gerichte ist eine Weitergabe daneben auch zu Zwecken der Beweismittellieferung in Zivilrechtsangelegenheiten, zB zur Klärung von Wegehalterhaftungen oder beim Verdacht der Kindesentziehung im Besuchs- und Obsorgestreit, zulässig. Eine Weitergabe an Versicherungen ist ausschließlich auf die Abwicklung konkreter Versicherungsfälle beschränkt.

4. Inhaltliche Rechtmäßigkeit der Videoüberwachung und Rechtsdurchsetzung

Da die DSK im Meldeverfahren lediglich die Zweckgebundenheit prüft, ist auch bei Erfüllung sämtlicher Voraussetzungen des Abschnitts F. der SA032 „Videoüberwachung" über die Rechtmäßigkeit der Datenanwendung, insb im Verhältnis zu den Betroffenen, keine automatische Unbedenklichkeit bescheinigt.

Vielmehr wirft die Verarbeitung von personenbezogenen Daten durch „ausländische Vertretungen und Internationale Organisationen" weitergehende Fragen auf, die – soweit ersichtlich – bislang weder in der österreichischen Fachliteratur noch in der Datenschutzpraxis behandelt worden sind.

4.1. Datenverarbeitung durch ausländische Vertretungsbehörden und Internationale Organisationen

Das Wiener Übereinkommen über diplomatische Beziehungen (WDK)[23] regelt als multilateraler Staatsvertrag grundsätzlich nur Rechte und Pflichten zwischen den Völkerrechtssubjekten untereinander, im konkreten Fall der Republik Österreich im Verhältnis zu anderen Völkerrechtssubjekten, die diplomatische Missionen in Österreich unterhalten. Art 31 und 32 WDK bestimmen die Immunität von Dip-

23) BGBl 66/1966.

lomaten. Nach Art 31 Abs 1 WDK genießt der Diplomat Immunität von der Strafgerichtsbarkeit des Empfangsstaats. Ferner steht ihm Immunität von dessen Zivil- und Verwaltungsgerichtsbarkeit[24] mit Ausnahme von taxativ aufgezählten Fällen zu, die für die datenschutzrechtlichen Zwecke der Videoüberwachung alle nicht einschlägig sind. Nach Art 31 Abs 4 WDK befreit die Immunität des Diplomaten diesen von der Gerichtsbarkeit des Empfangsstaates, nicht aber von der Gerichtsbarkeit des Entsendestaates. Nach hA[25] ist die Immunität ein Recht, das nicht dem Begünstigten sondern dem Entsendestaat zusteht, sodass auch nur dieser und nicht der Begünstigte darauf verzichten kann.

Dem Befund *Blumes*[26] ist beizupflichten, wonach Botschaften und andere ausländische Vertretungen, die von den Regeln des Völkerrechts über diplomatische Beziehungen abgedeckt werden, einen besonderen und unsicheren Ort für den Datenschutz darstellen. Auch wenn das Recht des Empfangsstaates zur Anwendung kommt, dh in den meisten europäischen Ländern würden die Standards der DSRL gelten, gibt es Schwierigkeiten mit der faktischen Anwendung dieser Regeln; In jedem Fall könnten sie nicht durchgesetzt werden. Der Datenschutz in diesem Bereich wird also unsicher. Die Regeln des Empfangsstaates sind von der jeweiligen diplomatischen Mission bloß freiwillig zu beachten, und es ist wahrscheinlich, dass dies nicht immer getan wird.[27]

4.2. Durchsetzung des Auskunftsrechts

Für die Auskunft über eine Videoüberwachung iSd § 50a Abs 1 DSG gelangen – neben den allgemeinen Bestimmungen des DSG – auch die Bestimmungen des Abschnittes 9a. zur Anwendung. § 50e Abs 1 DSG referenziert dafür ausdrücklich § 26 DSG in der Weise, dass die Form der Auskunftserteilung „abweichend von § 26 Abs 1" geregelt wird. Demnach ist die Auskunft primär durch Zurverfügungstellung einer Kopie der Videobildaufzeichnungen über den Auskunftswerber zu erteilen. Aus dem Umstand, dass § 50e DSG nur Abweichungen von § 26 DSG regelt, schließt die Spruchpraxis,[28] dass er keine völlig neue und eigenständige Art der Auskunft regelt, sondern das bereits gem § 26 DSG bestehende Auskunftsrecht für aufgezeichnete Bilddaten ergänzt und anpasst. Das Auskunftsrecht nach § 50e DSG reicht demnach nicht weiter als der Auskunftsanspruch nach § 26 DSG, sondern setzt diesen voraus. Für den Fall, dass keine Auswertung aus diesen Bilddaten stattgefunden hat, steht keine Auskunft zu.[29] Diese Ansicht der DSK steht im Widerspruch zu den Gesetzesmaterialien[30] der DSG-Nov 2010 und ist in der Lehre[31] bereits mit überzeugenden Argumenten kritisiert worden. Die Spruchpraxis hält aber nach wie vor daran fest.[32]

Für ausgewertete Videoaufzeichnungen, dh im Anlassfall, kommt hingegen der Auskunftsanspruch nach § 50e DSG vollinhaltlich zum Tragen.[33] Seine Durchsetzung stößt jedoch sehr rasch an völkerrechtliche Grenzen: Nach Art 22 Abs 3 und Art 31 WDK sind sämtliche Räumlichkeiten der Mission dem Zugriff durch Organe (Exekutivbeamte) des Empfangsstaats entzogen.[34] Unter „Exterritorialität" ist schließlich die Befreiung von Gerichtsbarkeit und Zwangsgewalt des Empfangsstaates zu verstehen.[35] Diesbezüglich sind insb die Art 29 ff WDK von Bedeutung. Nach diesen Bestimmungen ist die Person des Diplomaten unverletzlich. Er unterliegt keiner Festnahme oder Haft irgendwelcher Art. Weiters ist die Unverletzlichkeit seiner Privatwohnung und seiner Papiere und Korrespondenz festgelegt und die Immunität von der Strafgerichtsbarkeit des Empfangsstaates sowie weitgehend auch von dessen Zivil- und Verwaltungsgerichtsbarkeit. Die Unverletzlichkeit der Räumlichkeiten der Mission bedeutet auch die Immunität von jeglicher Vollstreckung.[36] Dies bedeutet allerdings mE keine „a limine" Zurückweisung eines Auskunftsbegehrens bei der DSK, da zumindest ein Rechtsschutzinteresse des Betroffenen an Erlangung einer Entscheidung besteht, auch wenn sie – bei einem Zusammenhang mit der offiziellen Tätigkeit des Staatenvertreters – nicht vollstreckbar ist.[37]

5. Zusammenfassung

Die mit 31. 3. 2011 in Kraft getretene Novelle der Standard- und Musterverordnung (StMV 2004) nimmt ua Videoüberwachungen ausländischer Vertretungen und Internationaler Organisationen von der Meldepflicht an die DSK aus, sofern davon lediglich Außenteile bzw Zutrittsbereiche der jeweiligen Missionsgebäude betroffen sind. Der Einsatz von optisch-technischen Hilfsmitteln oder Geräten[38] ist lediglich zum Eigentums- und Verantwortungsschutz sowie zur Vermeidung bzw Verfolgung strafbaren Verhaltens zulässig. Eine Überprüfung der inhaltlichen Rechtmäßigkeit der Datenverarbeitung und der Durchsetzung der Betroffenenrechte gestaltet sich aufgrund der völkerrechtlichen Exterritorialität der Auftraggeber mitunter äußerst schwierig.

24) In der authentischen Textfassung: *„Immunity from its civil and administrative jurisdiction"*.
25) VwGH 22. 12. 2000, 2000/12/0305, ZfVB 2002/584; *Neuhold/Hummer/Schreuer*, Handbuch I² Rz 1525 ff; unter Berufung auf die EB RV 738 BlgNR X. GP, 45.
26) *Peter Blume*, Embassies and Personal Data – An Unsafe Place for Data Protection, CRi 2011, 39, 43 f.
27) *Blume*, CRi 2011, 39, 44.
28) DSK 30. 7. 2010, K121.605/0014-DSK/2010, jusIT 2010, 187 (*König*).
29) Deutlich DSK 5. 12. 2008, K121.385/0007-DSK/2008, jusIT 2009/12, 24 zur alten Rechtslage.
30) Arg: „Abweichend von § 26 Abs 1 …", EBRV 472 BlgNR 24. GP, 20 abgedruckt in der Textausgabe *ProLibris*, DSG³ (2010), 202.
31) *Jahnel*, Handbuch Rz 7/27 und Rz 8/110.
32) DSK 30. 7. 2010, K121.605/0014-DSK/2010, jusIT 2010/89, 186.
33) Deutlich DSK 5. 12. 2008, K121.385/0007-DSK/2008, jusIT 2009/12, 24.
34) *Neuhold/Hummer/Schreuer*, Handbuch I² Rz 1527 f.
35) VwGH 2. 7. 2008, 2007/08/0207, ARD 5938/13/2009 = infas 2009, S 16 = EF-Z 2009/28, 30 (*Leitner*) = ZfVB 2009/1211/1294 = DRdA 2009, 430; 4. 7. 2005, 2003/10/0144, ZfVB 2006/1623/1650/1795/1804.
36) LGZ Wien 23. 3. 1999, 39 R 126/99i, MietSlg 51.615.
37) Vgl LGZ Wien 23. 3. 1999, 39 R 126/99i, MietSlg 51.615.
38) Dazu bereits *Thiele*, jusIT 2011, 14 f.

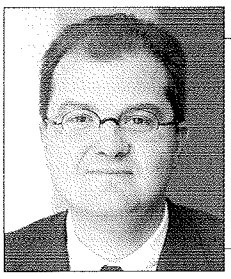
Foto D. Wild

Der Autor:
RA Dr. *Clemens Thiele*, LL.M. Tax (GGU), studierte US-amerikanisches Steuerrecht in San Francisco; Gründer der RA-Kanzlei EUROLAWYER® in Salzburg; Fachbuch-Autor; Verfasser des Standardkommentars zum Werbeabgabegesetz (2000); gerichtlich beeideter Sachverständiger für Urheberfragen aller Art, insb Neue Medien und Webdesign.

Publikationen des Autors:
Rechtssichere Verwendung von Schutzzeichen, RdW 2010/568, 557; Zero Intern – Rechtswidrige AGBs als Lauterkeitsverstoß, RdW 2010/424, 388; Urheberrecht und Erben, in: *Bogendorfer/Ciresa* (Hrsg), Urheberrecht (2009) 51; Co-Autor in *Triffterer/Rosbaud/Hinterhofer* (Hrsg), Salzburger Kommentar zum Strafgesetzbuch.