www.manz.at/rfg

RECHT & FINANZEN FÜR GEMEINDEN

RFG

Bericht: Future Village!

Herausgeber Walter Leiss
Schriftleitung und Redaktion Markus Achatz, Peter Pilz
Redaktion Christoph Grabenwarter, Ferdinand Kerschner, Katharina Pabel, Alfred Riedl, Ursula Stingl-Lösch

September 2019 **03**

77 – 136

Schwerpunkt

Finanzielle Risiken für Gemeinden

Übersicht

Beiträge

ISSN 1993-8098 Österreichische Post AG PZ 06Z036884 P Verlag Manz, Gutheil Schoder Gasse 17, 1230 Wien

MANZ

Videoüberwachung durch die öffentliche Hand

Einsatz der Videoüberwachung in der Hoheitsverwaltung und in der Privatwirtschaftsverwaltung

Von Marija Križanac

RFG 2019/25

§§ 12, 13 DSG; Art 6 DSGVO

Videoaufnahme; Bildaufnahme; Bildverarbeitung

Inhaltsübersicht:

A. Allgemeines

Die Datenschutz-Grundverordnung (DSGVO)[1] ist in aller Munde und bereitet vielen in der Praxis auch über ein Jahr nach Geltendwerdung noch Kopfzerbrechen. Ein wichtiger Praxisfall – die Videoüberwachung durch die öffentliche Hand – wird nachfolgend behandelt. Es wird erklärt, auf welcher Rechtsgrundlage und unter welchen Voraussetzungen die Videoüberwachung eingesetzt werden kann.

B. Rechtsgrundlage für die Videoüberwachung

1. Einordnung der Videoüberwachung im neuen Datenschutzrechts-Regime

a) Hoheitsverwaltung vs Privatwirtschaftsverwaltung

Die DSGVO wurde bewusst technologieneutral gehalten[2] und enthält daher keine Spezialbestimmungen zur Videoüberwachung. Anders das DSG – in den §§ 12 und 13 DSG wird die sog „Bildverarbeitung"[3] geregelt, worunter auch die Videoüberwachung fällt. Diesen Spezialbestimmungen unterfällt jedoch nur die Bildverarbeitung *„zu privaten Zwecken"*.[4] Hierunter fallen Videoüberwachungen von Verantwortlichen des privaten Bereichs, was auch Videoüberwachungen im Rahmen der **Privatwirtschaftsverwaltung** umfasst (zB Videoüberwachung von öffentlichen Gebäuden im Rahmen der Privatwirtschaftsverwaltung). Jedenfalls vom Anwendungsbereich der Spezialbestimmungen ausgenommen sind Videoüberwachungen zur Vollziehung hoheitlicher oder schlicht hoheitlicher Aufgaben.[5] Die Videoüberwachung im Rahmen der **Hoheitsverwaltung** muss somit nach den Regelungen der DSGVO[6] und nicht nach jenen der §§ 12 und 13 DSG beurteilt werden.[7]

b) Sensible Daten vs nicht-sensible Daten

Das Datenschutzrecht kennt verschiedene Arten von personenbezogenen Daten, für die mitunter unterschiedliche Vorschriften gelten. Unterschieden wird insb zwischen „regulären" personenbezogenen Daten und *„besonderen Kategorien personenbezogener Daten"* (gemeinhin auch „sensible Daten" genannt).[8]

Es besteht seit geraumer Zeit die Diskussion, welcher dieser beiden Arten von personenbezogenen Daten die Videoüberwachungsdaten zuzuordnen sind.[9] Die Videoüberwachung hält das physische Erscheinungsbild und Verhalten einer Person fest – von der rassischen und ethnischen Herkunft (zB Hautfarbe) und der religiösen oder weltanschaulichen Überzeugung (zB Kopftuch, Kippa) bis hin zu biometrischen Daten (zB Gesichtszüge) und Gesundheitsdaten (zB Rollstuhl, Gipsarm) könnten potenziell viele Informationen, die nach der DSGVO als sensibel gelten, aus Videoüberwachungsdaten „herausgelesen" werden.

In Österreich kann aufgrund der Rsp der Datenschutzbehörde davon ausgegangen werden, dass iZm der Videoüberwachung dennoch (jedenfalls im Allgemeinen und ohne Hinzutreten besonderer Umstände

1) VO (EU) 2016/679 des EP und des Rates v 27. 4. 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung – DSGVO), ABl L 2016/119, 1.
2) Vgl ErwGr 15 DSGVO.
3) Zur Frage der Unionsrechtskonformität dieser Regelungen, auf die im Rahmen dieses Beitrags nicht eingegangen wird, vgl etwa *Müllner/Wieser*, §§ 12f DSG – Kein Spielraum für Beharrlichkeit, jusIT 2019, 72.
4) § 12 Abs 1 DSG.
5) ErläutAB 1664 BlgNR 25. GP 14.
6) Für die hoheitsverwaltungsrechtliche Videoüberwachung zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten sind die Richtlinie (EU) 2016/680 des EP und des Rates v 27. 4. 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl L 2016/119, 89; in Österreich umgesetzt in §§ 31ff DSG – sowie die jeweiligen Materiengesetze (zB SPG, StPO) einschlägig. Vgl auch *EDSA*, Guidelines 3/2019 on processing of personal data through video devices v 10. 7. 2019, Rz 10.
7) Sie bedarf zudem einer gesetzlichen Rechtsgrundlage (§ 1 DSG, Art 18 B-VG), vgl ErläutAB 1664 BlgNR 25. GP 14 (dazu sogleich).
8) Art 9 Abs 1 DSGVO.
9) Vgl zu dieser Diskussion etwa *Knyrim*, Bilddaten: immer sensibel? jusIT 2016, 235 und *Bergauer*, Die Einordnung von Bilddaten erkennbarer Personen im Datenschutzrecht. Eine Replik auf *Knyrim*, Bilddaten: immer sensibel? jusIT 2016, 235, jusIT 2016, 241.

und Zwecke) **keine Verarbeitung besonderer Kategorien personenbezogener Daten** vorliegt.[10]

Auch der Europäische Datenschutzausschuss **(EDSA)** scheint diese Ansicht zu vertreten; in seinen Leitlinien zur Videoüberwachung hält der EDSA fest, dass die Videoüberwachung nicht immer als eine Verarbeitung besonderer Kategorien personenbezogener Daten zu betrachten sei, sehe man auf den Aufnahmen etwa, dass jemand eine Brille trägt oder im Rollstuhl sitzt, handle es sich dabei nicht per se um sensible Daten. Werden die Aufnahmen aber nach solchen sensiblen Kriterien ausgewertet, liege eine Verarbeitung besonderer Kategorien personenbezogener Daten vor.[11]

2. Mögliche Erlaubnistatbestände

a) Hoheitsverwaltung

Auf Basis der obigen Einordnung ist für die Videoüberwachung im Rahmen der Hoheitsverwaltung Art 6 DSGVO einschlägig;[12] es kommen insb die folgenden Erlaubnistatbestände in Frage:

➜ **Die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt:**[13]

Die Rechtsgrundlage für eine solche Verarbeitung ergibt sich entweder aus dem Unionsrecht oder aus dem nationalen Recht.[14]

Nach den Vorstellungen des Gesetzgebers muss in dieser gesetzlichen Rechtsgrundlage ausdrücklich auf die Videoüberwachung Bezug genommen werden, dh es ist ein Materiengesetz erforderlich, das den Einsatz der Videoüberwachung regelt.[15]

Beispiele

Ein Beispiel hierfür ist etwa der Einsatz der Videoüberwachung bei der Verkehrsbeobachtung gem § 98 f StVO.

Viele hoheitliche Aufgaben, die eine Videoüberwachung erfordern bzw erlauben, sind **Sicherheitsbehörden vorbehalten**[16]; zB die Videoüberwachung zur **Vorbeugung befürchteter gefährlicher Angriffe**[17] **an öffentlichen Orten**[18] gegen Leben, Gesundheit oder Eigentum von Menschen (insb, wenn eine solche Befürchtung wegen vorangegangener gefährlicher Angriffe besteht).[19] Dies bedeutet, dass Sicherheitsbehörden zur präventiven Videoüberwachung an „Kriminalitätsbrennpunkten" ermächtigt sind.[20] Zu denken ist etwa an bekannte Plätze für Suchtgifthandel, Parks bei gefährlichen Angriffen gegen Frauen.[21] Anderen Hoheitsträgern bleibt eine solche Videoüberwachung verwehrt.[22]

➜ **Die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich:**[23]

Es gilt das soeben Gesagte. Anders als bei den Aufgaben im öffentlichen Interesse/in Ausübung öffentlicher Gewalt muss hier nicht nur eine Erlaubnis, sondern eine Verpflichtung zur Videoüberwachung bestehen. Es gibt nur wenige gesetzliche Regelungen, die eine Videoüberwachung verpflichtend vorschreiben, zB

Beispiele

§ 4 Abs 5 Straßentunnel-SicherheitsG, der den Tunnel-Manager[24] dazu verpflichtet, in allen Tunneln, die von einer Überwachungszentrale überwacht werden, zur automatischen Erkennung von Verkehrsstörungen ein Videoüberwachungssystem zu betreiben;

§ 13 Informationssicherheitsverordnung, die Dienststellen des Bundes zur Einführung von Maßnahmen zur physischen Absicherung der Räumlichkeiten, in denen klassifizierte Informationen aufbewahrt werden, verpflichtet. Zu diesen Maßnahmen kann, auf der Grundlage einer Einschätzung der Bedrohungslage durch die zuständigen Behörden, auch die Videoüberwachung zählen.

Zu betonen ist, dass sich Hoheitsträger bei der Videoüberwachung im Rahmen der Hoheitsverwaltung jedenfalls **nicht auf folgende Erlaubnistatbestände stützen können:**

10) Vgl DSB 7. 6. 2018, DSB-D202.207/0001-DSB/2018: *„Die ehemalige Datenschutzkommission hat bereits mehrfach festgestellt, dass Bilddaten (bestimmbare) personenbezogene Daten sind (vgl etwa die Ausführungen zum ehemaligen § 4 Z DSG 2000 im Bescheid der DSK vom 21. 1. 2009, GZ K121.425/0003-DSK/2009). Diese Erwägungen lassen sich auch auf Art 4 Z 1 DSGVO umlegen. Die DSGVO ist somit einschlägig.* ***Gleichzeitig liegt mit diesen Bilddaten aber keine Verarbeitung besonderer Kategorien personenbezogener Daten iSd Art 9 DSGVO vor*** *(vgl die Ausführungen zum ehemaligen § 4 Z 2 DSG 2000, den Bescheid der DSK vom 10. 4. 2013, GZ K202.120/0002-DSK/2013)"* (Hervorhebung durch die Autorin dieses Beitrags).

11) *EDSA*, Guidelines 3/2019 on processing of personal data through video devices v 10. 7. 2019, Rz 60 ff. Im Zeitpunkt der Fertigstellung dieses Beitrags befanden sich diese Leitlinien im Stadium der öffentlichen Konsultation.

12) Vgl jedoch FN 7 zur RL (EU) 2016/80.

13) Art 6 Abs 1 lit e DSGVO.

14) Art 6 Abs 3 DSGVO.

15) ErläutAB 1664 BlgNR 25. GP 14; vgl bereits ErläutRV 472 BlgNR 24. GP 18 und 19.

16) Hier ist zudem grundsätzlich nicht die DSGVO, sondern sind die §§ 36 ff DSG einschlägig, vgl bereits FN 7 zu RL (EU) 2016/680.

17) Ein gefährlicher Angriff ist (i) die Bedrohung eines Rechtsguts durch die rechtswidrige Verwirklichung des Tatbestands einer gerichtlich strafbaren Handlung, die vorsätzlich begangen und nicht bloß auf Verlangen eines Verletzten verfolgt wird, und (ii) ein Verhalten, das darauf abzielt und geeignet ist, eine solche Bedrohung vorzubereiten, sofern dieses Verhalten in engen zeitlichen Zusammenhang mit der angestrebten Tatbestandsverwirklichung gesetzt wird, vgl § 16 Abs 2 und 3 SPG.

18) Öffentliche Orte sind solche, die von einem nicht von vornherein bestimmten Personenkreis betreten werden können; vgl § 27 Abs 2 SPG.

19) § 54 Abs 6 SPG. Ein weiteres Beispiel sind etwa die Befugnisse der Kriminalpolizei bzw Staatsanwaltschaft zur optischen und akustischen Überwachung von Personen gem § 136 StPO.

20) *Weiss* in *Thanner/Vogl* (Hrsg), SPG² § 54 Anm 44.

21) Vgl ErläutRV 643 BlgNR 22. GP 11.

22) Vgl etwa DSK 21. 6. 2005, K503.425-090/0003-DVR/2005. Der Magistrat der Stadt Villach versuchte damals noch bei der Datenschutzkommission eine Registrierung folgender Datenanwendung: *„Videoüberwachung an öffentlichen Orten, an denen zu befürchten ist, dass es zu gefährlichen Angriffen gegen Leben, Gesundheit oder Eigentum von Menschen kommen wird; Ermittlung personenbezogener Daten Anwesender mit Bild- und Tonaufzeichnungsgeräten zur Vorbeugung gefährlicher Angriffe und Aufklärung strafrechtlich relevanter Sachverhalte"*. Als Rechtsgrundlage führte der Magistrat der Stadt Villach ua die Unterstützung der Sicherheitsbehörden bei der Vollziehung des SPG an. Dies ließ die Datenschutzkommission ua mangels Zuständigkeit nicht gelten und wies die Registrierung ab.

23) Art 6 Abs 1 lit c DSGVO.

24) Straßenerhalter der Bundesstraße, vgl § 2 Z 4 Straßentunnel-SicherheitsG.

➜ **Die Verarbeitung ist zur Wahrung berechtigter Interessen erforderlich:**[25]

In Art 6 Abs 1 lit f Unterabsatz 1 DSGVO wird klargestellt, dass dieser in der Praxis so wichtige Erlaubnistatbestand nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung personenbezogener Daten gilt. Begründet wird dies damit, dass es dem jeweiligen nationalen Gesetzgeber obliegt, mittels einer Rechtsvorschrift die Grundlage für eine solche Verarbeitung zu schaffen.[26]

➜ **Die betroffene Person hat ihre Einwilligung gegeben:**[27]

Dasselbe muss auch iZm der Einwilligung gelten. Wurde der hoheitlich handelnde Akteur nicht gesetzlich zur Videoüberwachung berechtigt oder verpflichtet, kann er diese nicht auf Basis einer Einwilligung dennoch durchführen.[28]

b) Privatwirtschaftsverwaltung

Wie eingangs erwähnt, gelten bei der Videoüberwachung im Rahmen der Privatwirtschaftsverwaltung die Spezialbestimmungen der §§ 12 und 13 DSG. In § 12 Abs 2 DSG werden zunächst generelle Erlaubnistatbestände, die jenen des Art 6 Abs 1 DSGVO ähneln, beschrieben. Erwähnenswert sind insb die nachstehenden:

➜ **Einwilligung der betroffenen Personen:**

Anders als bei der Videoüberwachung im Rahmen der Hoheitsverwaltung ist eine Berufung auf den Erlaubnistatbestand der Einwilligung hier möglich.[29]

Praxistipp

Gerade im Bereich der Videoüberwachung ist dieser Einwilligungstatbestand jedoch nicht besonders praktikabel, da idR ein unbestimmter Personenkreis davon betroffen ist und somit eine Einholung von Einwilligungserklärungen oftmals nicht möglich sein wird; zudem ist die Einwilligung jederzeit widerrufbar. Es empfiehlt sich daher nicht, eine Videoüberwachung auf die Einwilligung der betroffenen Personen zu stützen.

➜ **Besondere gesetzliche Bestimmungen, die eine Bildaufnahme anordnen oder erlauben:**

Hier gilt das oben zu Art 6 Abs 1 lit c und e DSGVO Gesagte.

➜ **Überwiegende berechtigte Interessen des Verantwortlichen oder eines Dritten:**

In der Praxis ist dies der wichtigste Erlaubnistatbestand für die Videoüberwachung im Rahmen der Privatwirtschaftsverwaltung.

Der Gesetzgeber hat in § 12 Abs 3 DSG diese Interessenabwägung für bestimmte Fälle bereits auf gesetzlicher Ebene vorgenommen und bestimmt, dass die Bildaufnahme in diesen Fällen jedenfalls zulässig ist.

Beispiele

Für die Videoüberwachung im Rahmen der Privatwirtschaftsverwaltung ist der folgende Fall relevant: Die Bildverarbeitung ist für den **vorbeugenden Schutz von Personen oder Sachen an öffentlich zugänglichen Orten,** die dem **Hausrecht** des Verantwortlichen unterliegen, erforderlich; dies aufgrund **bereits erfolgter Rechtsverletzungen** oder eines in der Natur des Ortes liegenden **besonderen Gefährdungspotenzials.**[30] Darunter fällt zB die Videoüberwachung von öffentlichen Verkehrsmitteln (Schutz vor Vandalismus, Sachbeschädigung; Schutz der Fahrgäste) und von Verwaltungsgebäuden und öffentlichen Einrichtungen wie Museen udgl (Schutz vor Vandalismus, Einbruch; Schutz der Beschäftigten, Wegehalterpflichten).[31]

Die Liste in Abs 3 ist nicht abschließend (Arg „insbesondere"); im Rahmen einer Interessenabwägung können auch andere Fälle der Videoüberwachung gerechtfertigt sein.

Anders als Art 6 Abs 1 lit f DSGVO lässt § 12 Abs 2 DSG nicht ein Gleichgewicht der Interessen genügen, sondern fordert, dass die Interessen des Verantwortlichen (oder eines Dritten) **schwerer wiegen** als jene der betroffenen Personen.[32]

Praxistipp

Um der Rechenschaftspflicht des Art 5 Abs 2 DSGVO nachzukommen, empfiehlt es sich, diese Interessenabwägung schriftlich festzuhalten.[33]

Eine Videoüberwachung ist in den in § 12 Abs 4 DSG beschriebenen Fällen jedenfalls unzulässig, zB im höchstpersönlichen Lebensbereich ohne ausdrückliche Einwilligung (WCs, Umkleidekabinen etc), zur Mitarbeiterkontrolle und zur Auswertung anhand von sensiblen Kriterien (dunkle Hautfarbe, Kopftuch etc).

Klarstellend sei festgehalten, dass die Beschränkung auf vom Hausrecht iwS umfasste Orte nicht nur für den Fall des § 12 Abs 3 Z 2 DSG, sondern generell gilt – Videoüberwachung durch Private (dazu zählt auch die Videoüberwachung im Rahmen der Privatwirtschaftsverwaltung) **darf grundsätzlich nicht den öffentlichen Raum (Straßen, Gehsteige, Plätze etc) umfassen.**[34] Nur in Ausnahmefällen ist es zulässig,

25) Art 6 Abs 1 lit f DSGVO.
26) Vgl ErwGr 47 DSGVO. Dies gilt nicht im Bereich der Privatwirtschaftsverwaltung, vgl *Graf/Križanac*, „Datenschutz neu" für Gemeinden, RFG-Schriftenreihe, 4/2017, 15 ff; zuletzt erneut bestätigt in DSB 15. 11. 2018, DSB-D122.944/0007-DSB/2018.
27) Art 6 Abs 1 lit a DSGVO.
28) Dies gilt nicht im Rahmen der Privatwirtschaftsverwaltung. Vgl *Graf/Križanac*, „Datenschutz neu" für Gemeinden, RFG-Schriftenreihe 4/2017, 17.
29) Näheres zB in *Graf/Križanac*, „Datenschutz neu" für Gemeinden, RFG-Schriftenreihe 4/2017, 17 ff.
30) § 12 Abs 3 Z 2 DSG. Ähnlich auch *EDSA*, Guidelines 3/2019 on processing of personal data through video devices v 10. 7. 2019, Rz 18 ff.
31) Vgl dazu auch ErläutAB 1664 BlgNR 25. GP 14.
32) Auch abseits der Bestimmung des § 12 Abs 2 DSG wäre es in Anbetracht des Widerspruchsrechts nach Art 21 DSGVO sinnvoll, eine Videoüberwachung erst bei Überwiegen der berechtigten Interessen zu betreiben.
33) Idealerweise orientiert man sich hierbei am Prüfschema der Art. 29-Datenschutzgruppe, vgl Stellungnahme 06/2014 zum Begriff des berechtigen Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG (WP 217) v 9. 4. 2014. Vgl auch EDSA, Guidelines 3/2019 on processing of personal data through video devices v 10. 7. 2019, Rz 30 ff.
34) Vgl Erläut zum Entwurf der DSFA-AV v 21. 3. 2018, 3; abrufbar unter www.dsb.gv.at/documents/22758/116802/Verordnung_der_

dass an das überwachte Objekt angrenzende Randbereiche des öffentlichen Raums miterfasst werden, dies jedoch nur unter größtmöglicher Schonung unbeteiligter Dritter.[35]

Beispiele

ZB indem die Kamera bei einer Gebäudeüberwachung so ausgerichtet wird, dass sie den angrenzenden Gehsteig nur so wenig wie möglich erfasst, oder durch automatische Verpixelung der für den Zweck der Videoüberwachung nicht relevanten Bereiche.[36]

C. Pflichten iZm einer Videoüberwachung

Nachfolgend werden spezielle Pflichten iZm der Videoüberwachung sowie allgemeine Pflichten, die bei der Videoüberwachung Besonderheiten aufweisen, erörtert.

Dieser Beitrag befasst sich nicht mit sonstigen allgemeinen Pflichten eines Verantwortlichen.[37]

1. Notwendige Maßnahmen, Kennzeichnung

Bei der Videoüberwachung im Rahmen der Privatwirtschaftsverwaltung sind die Spezialbestimmungen des § 13 DSG zu beachten.

Der Verantwortliche ist verpflichtet,

- geeignete Datensicherheitsmaßnahmen zu implementieren und sicherzustellen, dass Unbefugte keinen Zugang haben und keine nachträglichen Veränderungen der Aufnahmen vornehmen können (zB Verschlüsselung, Zugangsbeschränkungen etc);[38]
- jeden Verarbeitungsvorgang iZm der Videoüberwachung zu protokollieren (außer in den Fällen einer Echtzeitüberwachung);[39]
- die Aufnahmen zu löschen, sobald sie für den Zweck, für den sie aufgenommen wurden, nicht mehr benötigt werden und keine gesetzliche Aufbewahrungspflicht besteht. Sollen die Aufnahmen länger als 72 Stunden aufbewahrt werden, muss diese längere Aufbewahrung verhältnismäßig sein und gesondert protokolliert und begründet werden;[40]
- die Videoüberwachung geeignet zu kennzeichnen. Aus der Kennzeichnung muss jedenfalls der Verantwortliche hervorgehen (es sei denn, dieser ist den betroffenen Personen nach den Umständen des Falls bereits bekannt).[41]

Praxistipp

In der Praxis hat es sich eingebürgert, für die Kennzeichnung ein Hinweisschild, auf dem ein Piktogramm abgebildet ist (zB das Piktogramm „Videoüberwachung" nach DIN 33450), zu verwenden.

Praxistipp

Die Kennzeichnung der Videoüberwachung **entbindet nicht** von den sonstigen **Informationspflichten** nach Art 13 DSGVO – zusätzlich zur Kennzeichnung ist den betroffenen Personen auch eine alle Pflichtangaben nach Art 13 DSGVO beinhaltende Datenschutzerklärung zur Verfügung zu stellen. Hierzu kann zB auf dem Hinweisschild ein Link oder ein QR-Code, der zur Datenschutzerklärung führt, angebracht werden. Zusätzlich empfiehlt es sich, die Datenschutzerklärung auch physisch aufliegen zu haben (etwa als Aushang im Eingangsbereich eines überwachten Gebäudes).[42]

Diese Pflichten fußen auf allgemeinen Grundsätzen[43] und Pflichten[44] nach der DSGVO und können daher auch im Rahmen der Hoheitsverwaltung als Orientierungshilfe für den DSGVO-konformen Einsatz der Videoüberwachung herangezogen werden.

2. Auswertung, Löschung

Die Grundsätze der Zweckbindung und Datenminimierung[45] bedeuten iZm der Videoüberwachung, dass die Überwachungsaufnahmen nur in im Vorhinein festgelegten (dh zweckbezogenen) Anlassfällen gesichtet/ausgewertet werden dürfen und ansonsten nach Ablauf der festgelegten Aufbewahrungsdauer ungesichtet zu löschen sind.

Beispiele

Typische Zwecke sind bspw der Eigenschutz (zB Schutz des Eigentums, Schutz der Mitarbeiter), der Verantwortungsschutz (zB Wahrnehmung von Verkehrssicherungspflichten, Wegehalterpflichten) und Verhinderung/Eindämmung/Aufklärung strafrechtlich relevanten Verhaltens, soweit dieses den Verantwortlichen betrifft (zB Einbruch in das überwachte Objekt, Sachbeschädigung am überwachten Objekt).[46]

Datenschutzbeh%c3%b6rde_%c3%bcber_die_Ausnahmen_von_der_Datenschutz-Folgenabsch%c3%a4tzung_DSFA-AV__Erl%c3%a4uterungen.pdf/83514f8f-592c-438d-9bbb-fa2d0d9e16b9 (Stand 16. 7. 2019). Anderes gilt freilich im Rahmen der **Hoheitsverwaltung,** wenn eine solche Überwachung des öffentlichen Raums gesetzlich vorgesehen ist, vgl etwa die Befugnis der Sicherheitsbehörden in § 54 Abs 6 SPG.

35) Erläut zum Entwurf der DSFA-AV v 21. 3. 2018, 3.

36) Vgl *EDSA*, Guidelines 3/2019 on processing of personal data through video devices v 10. 7. 2019, Rz 27.

37) ZB Pflicht zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten gem Art 30 DSGVO; Pflicht zum Abschluss eines Auftragsverarbeitungsvertrags gem Art 28 DSGVO, wenn ein Dritter (zB ein Sicherheitsunternehmen) mit der Videoüberwachung beauftragt wird.

38) § 13 Abs 1 DSG. Vgl auch *EDSA*, Guidelines 3/2019 on processing of personal data through video devices v 10. 7. 2019, Rz 121 ff zu Maßnahmen, die der EDSA empfiehlt.

39) § 13 Abs 2 DSG.

40) § 13 Abs 3 DSG.

41) § 13 Abs 5 DSG. Zur Kennzeichnung s auch *EDSA*, Guidelines 3/2019 on processing of personal data through video devices v 10. 7. 2019, Rz 112 ff.

42) Vgl *EDSA*, Guidelines 3/2019 on processing of personal data through video devices v 10. 7. 2019, Rz 108 ff.

43) Vgl Art 5 DSGVO, zB Transparenz, Zweckbindung, Speicherbegrenzung.

44) Vgl Löschungspflicht nach Art 17 DSGVO, Pflicht zur Setzung von Datensicherheitsmaßnahmen nach Art 32 DSGVO.

45) Art 5 Abs 1 lit b und c DSGVO.

46) Vgl SA032 der aufgehobenen Verordnung des Bundeskanzlers über Standard- und Musteranwendungen nach dem Datenschutzgesetz 2000 (Standard- und Muster-Verordnung 2004 – StMV 2004), BGBl II 2004/312.

3. Datenschutz-Folgenabschätzung

Nach der DSGVO muss der Verantwortliche bei einer Verarbeitung, die voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, vorab eine Abschätzung der Folgen der Verarbeitungsvorgänge für den Schutz der personenbezogenen Daten durchführen (Datenschutz-Folgenabschätzung).[47]

In Umsetzung des Art 35 Abs 4 und 5 DSGVO hat die DSB zwei Verordnungen erlassen – die DSFA-V[48] und die DSFA-AV[49] –, die dem Rechtsanwender bei der Beurteilung helfen, ob eine Datenschutz-Folgenabschätzung durchzuführen ist oder nicht.

In Bezug auf die Videoüberwachung hat die DSB in der DSFA-AV zwei Ausnahmen vorgesehen:

Stationäre Bildverarbeitung und die damit verbundene Akustikverarbeitung zu Überwachungszwecken (Videoüberwachung):[50]

- Hierunter fallen Videoüberwachungen, die für den **vorbeugenden Schutz von Personen oder Sachen** an **allgemein zugänglichen Orten,** die dem **Hausrecht** des Verantwortlichen unterliegen, aufgrund bereits erfolgter Rechtsverletzungen oder eines in der Natur des Ortes liegenden besonderen Gefährdungspotenzials erforderlich sind. „Allgemein zugängliche Orte" sind insb Eingangsbereiche/Foyers eines Objekts, aber zB nicht Büros im Inneren[51] oder WCs/Umkleidekabinen.[52]
- Diese Ausnahme gilt nicht für Örtlichkeiten, welche aufgrund eines bestehenden Kontrahierungszwangs oder aufgrund des öffentlichen Interesses von jedermann betreten werden dürfen – dies betrifft zB Verkehrseinrichtungen (öffentliche Verkehrsmittel) und Spitäler. **Öffentliche Verwaltungsgebäude** (zB Gemeindeämter) sind davon nicht betroffen; in den Erläut zur DSFA-AV wird klargestellt, dass die Ausnahme von der Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung auch für Videoüberwachungen von öffentlichen Verwaltungsgebäuden mit gültiger Zustimmung der Personalvertretung gilt.[53]
- Die Ausnahme gilt weiters auch für **Sportstätten, Freizeiteinrichtungen, Kultureinrichtungen** oder dergleichen.[54]
- Diese Art der Videoüberwachung bedarf keiner Datenschutz-Folgenabschätzung, wenn
  - nur Örtlichkeiten erfasst werden, über welche der Verantwortliche verfügungsbefugt ist. Die Videoüberwachung darf räumlich nicht über die Liegenschaft hinausreichen, mit Ausnahme einer zur Zweckerreichung allenfalls unvermeidbaren Einbeziehung öffentlicher Verkehrsflächen im Ausmaß von bis zu einem halben Meter, gemessen von der Grundstücksgrenze des überwachten Objekts. Die Videoüberwachung darf überdies nicht an Orten betrieben werden, welche den höchstpersönlichen Lebensbereich von Personen darstellen (zB WCs, Umkleidekabinen);
  - eine gültige Betriebsvereinbarung oder eine gültige Zustimmung der Personalvertretung, welche die Durchführung der Videoüberwachung regeln, vorliegt (wenn Beschäftigte zum Kreis der von der Videoüberwachung betroffenen Personen gehören);
  - die Aufnahmen spätestens nach 72 Stunden gelöscht werden (es sei denn, eine längere Speicherdauer wurde in einem Gesetz, durch einen behördlichen Rechtsakt, in einer Betriebsvereinbarung oder mit Zustimmung der Personalvertretung ausdrücklich festgelegt).

Bild- und Akustikdatenverarbeitung in Echtzeit:[55]

- Hierunter fallen **Videoüberwachungen in Echtzeit ohne Aufzeichnung.** Diese Art der Videoüberwachung bedarf keiner Datenschutz-Folgenabschätzung, wenn nur Örtlichkeiten erfasst werden, über die der Verantwortliche verfügungsbefugt ist. Die Videoüberwachung darf räumlich nicht darüber hinausreichen, mit Ausnahme einer zur Zweckerreichung allenfalls unvermeidbaren Einbeziehung öffentlicher Verkehrsflächen im Ausmaß von bis zu einem halben Meter. Orte, welche den höchstpersönlichen Lebensbereich von Personen darstellen (WCs, Umkleidekabinen), dürfen nicht erfasst werden.
- Ebenfalls von der Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung ausgenommen sind Videoüberwachungen, die nach der alten Rechtslage
  - der Vorabkontrolle durch die DSB unterlagen und vor Ablauf des 24. 5. 2018 im DVR registriert wurden oder
  - nicht meldepflichtig waren, dh der Standardanwendung SA032 der StMV 2004 entsprechen.[56]

Bei allen anderen Videoüberwachungen ist anhand des in der DSFA-V aufgestellten Kriterienkatalogs zu beurteilen, ob eine Datenschutz-Folgenabschätzung durchzuführen ist.[57]

Im Rahmen der Hoheitsverwaltung wird in der Regel die Ausnahme des Art 35 Abs 10 DSGVO zur Anwendung kommen und eine Datenschutz-Folgenabschätzung nicht erforderlich sein. ➜

47) Art 35 DSGVO.
48) V der Datenschutzbehörde über Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist, BGBl II 2018/278.
49) V der Datenschutzbehörde über die Ausnahmen von der Datenschutz-Folgenabschätzung, BGBl II 2018/108.
50) DSFA-A09.
51) Vgl dazu auch das Verbot der Videoüberwachung zum Zweck der Mitarbeiterkontrolle in § 12 Abs 4 Z 2 DSG.
52) Vgl dazu auch das Verbot der Videoaufnahme im höchstpersönlichen Lebensbereich in § 12 Abs 4 Z 1 DSG.
53) Erläut zum Entwurf der DSFA-AV v 21. 3. 2018, 3. Die Anwendbarkeit der Ausnahme auf Verwaltungsgebäude war zunächst nicht eindeutig, da in den Erläut zur DSVA-V bspw Ämter und Behörden als „Örtlichkeiten, die aufgrund eines öffentlichen Interesses von jedermann betreten werden dürfen", genannt werden, vgl Erläut zur DSFA-V, 3; abrufbar unter www.dsb.gv.at/documents/22758/116802/Erl%c3%a4uterungen+zur+DSFA-V.pdf/f488e164-f4f7-47d8-b218-167e83be1a10 (Stand 16. 7. 2019). Aus der Beantwortung einer diesbezüglichen Anfrage des Österreichischen Gemeindebundes durch die DSB ergibt sich jedoch, dass – entgegen dieser Widersprüchlichkeit – die Ausnahme generell für Verwaltungsgebäude gilt (Beantwortung auszugsweise wiedergegeben in *Haubenberger,* Videoüberwachung und Datenschutz, abrufbar unter www.kommunalnet.at/news/einzelansicht/videoueberwachung-und-datenschutz/news/detail.html [Stand 16. 7. 2019]).
54) Erläut zum Entwurf der DSFA-AV v 21. 3. 2018, 3.
55) DSFA-A10.
56) § 1 Abs 2 DSFA-AV.
57) Vgl § 2 Abs 2 und 3 DSFA-V.

4. Auskunftsrecht

Grundsätzlich hat eine betroffene Person ein Auskunftsrecht gegenüber dem Verantwortlichen – auf Anfrage ist der Verantwortliche verpflichtet, der betroffenen Person mitzuteilen, ob sie betreffende personenbezogene Daten verarbeitet werden. Ist dies der Fall, muss der Verantwortliche auch Auskunft über die verarbeiteten personenbezogenen Daten (inkl einer Kopie der personenbezogenen Daten) geben und diverse weitere Informationen zur Verfügung stellen.[58]

Gerade bei der Videoüberwachung ist der Verantwortliche oftmals nicht in der Lage, die Personen, die von der Videoüberwachung erfasst werden, zu identifizieren; eine solche Identifizierung ist für den Zweck, für den die Videoüberwachung eingesetzt wird, idR auch nicht erforderlich – zumeist (dh wenn kein zweckbezogener Anlassfall für eine Auswertung vorliegt) werden die Aufnahmen einer Videoüberwachung ungesichtet gelöscht.

Richtet eine Person in Bezug auf die Videoüberwachung ein Auskunftsersuchen an den Verantwortlichen, ist dieser nicht verpflichtet, Schritte zur Identifizierung dieser Person in seinem Videodatenbestand zu setzen (zB die Aufnahmen zu sichten), **es sei denn** die Person stellt dem Verantwortlichen **zusätzliche Informationen** zur Verfügung, die dem Verantwortlichen eine Identifizierung ermöglichen (zB Datum und Zeit, an dem/zu der die Person davon ausgeht, von der Videoüberwachung erfasst worden zu sein). Bei der Auskunftserteilung ist jedoch darauf zu achten, dass Rechte anderer betroffener Personen nicht verletzt werden (zB wenn die betroffene Person eine Kopie der Videoüberwachungsaufnahme verlangt: durch Verpixelung anderer erkennbarer Personen).[59] Der Verantwortliche ist auch nicht verpflichtet, die Aufnahmen aufzubewahren, nur um allfälligen Auskunftsersuchen nachkommen zu können. Ist der Verantwortliche auch mit den zusätzlichen Informationen der Person nicht in der Lage, diese zu identifizieren, finden die Betroffenenrechte in Art 15 bis 20 DSGVO keine Anwendung.[60] Diesfalls sollte der Verantwortliche die betroffene Person hierüber entsprechend informieren, dh der betroffenen Person mitteilen, dass er sie auch mit den zusätzlichen Informationen nicht identifizieren kann.[61]

58) Art 15 Abs 1 und 2 DSGVO.
59) Vgl *EDSA*, Guidelines 3/2019 on processing of personal data through video devices v 10. 7. 2019, Rz 93.
60) Art 11 DSGVO.
61) Vgl *EDSA*, Guidelines 3/2019 on processing of personal data through video devices v 10. 7. 2019, Rz 95.

➜ Zum Thema

Über die Autorin:
RA Mag. Marija Križanac, CIPP/E CIPM, leitet das Datenschutzrechts-Team der Graf & Pitkowitz Rechtsanwälte GmbH.
Kontaktadresse: Stadiongasse 2, 1010 Wien.
Tel: +43 (0)1 401 17 0, Fax: +43 (0)1 401 17 40
E-Mail: m.krizanac@gpp.at
Internet: www.gpp.at
Von derselben Autorin erschienen:
Graf/Križanac, „Datenschutz neu" für Gemeinden, RFG-Schriftenreihe 4/2017.
Danksagung:
Die Autorin dankt RA Dr. *Ferdinand Graf*, LL.M (NYU), für die wertvolle Unterstützung beim Verfassen dieses Beitrags.

➜ Literatur-Tipp

Datenschutz konkret, Kennenlernabo: 2 Hefte EUR 15,– dako.manz.at

MANZ Bestellservice:
Tel: (01) 531 61-100
Fax: (01) 531 61-455
E-Mail: bestellen@manz.at
Besuchen Sie unseren Webshop unter www.manz.at