

DIE REGELUNG DER VIDEOÜBERWACHUNG NACH DER DS-GVO

Gernot Fritz

Rechtsanwalt, Freshfields Bruckhaus Deringer LLP
Seilergasse 16, 1010 Wien, AT
gernotfritz@gmx.at

Schlagworte: *Videoüberwachung, Datenschutzgrundverordnung, DS-GVO, DSGVO, Bilddaten, Lichtbilder, sensible Daten*

Abstract: *Die DS-GVO enthält (im Gegensatz zum österreichischen DSG) keine Sonderregeln zur Videoüberwachung. Der vorliegende Beitrag beschäftigt sich mit den auf Videoüberwachungsaktivitäten anwendbaren Vorgaben der DS-GVO, insbesondere wie Videoüberwachungen in Zukunft datenschutzrechtlich gerechtfertigt werden können, ob es sich bei Lichtbildern nach den Vorgaben der DSGVO immer um sensible Daten handeln muss, und die Ausgestaltung und Durchsetzbarkeit der Betroffenenrechte bei Videoüberwachungsaktivitäten.*

1. Einleitung¹

Am 4. Mai 2016 wurde die Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutzgrundverordnung – **DS-GVO**) im Amtsblatt der Europäischen Union verkündet (Amtsblatt L119/1). Die DS-GVO ist am 25. Mai 2016 in Kraft getreten² und ist ab 25. Mai 2018 unmittelbar und unionsweit anwendbar.³ Die DS-GVO wird die nationalen Datenschutzgesetze der EU-Mitgliedstaaten – und somit auch das österreichische Datenschutzrecht – in weiten Teilen⁴ ablösen.

Im geltenden österreichischen Datenschutzgesetz 2000 (DSG) sind Videoüberwachungstätigkeiten (teilweise) im Abschnitt 9a (in den §§ 50a–50e) geregelt. Im Gegensatz zum geltenden Datenschutzrecht enthält die DSGVO allerdings keine Sonderregeln für Videoüberwachungstätigkeiten mehr. Für alle Datenverarbeitungen im Rahmen von Videoüberwachungstätigkeiten gelten somit die allgemeinen Regelungen der DS-GVO. Der vorliegende Beitrag stellt die auf Videoüberwachungstätigkeiten anwendbaren Rechtsnormen der DSGVO überblicksmäßig (und ohne Anspruch auf Vollständigkeit) dar⁵ und hebt bei den besprochenen Punkten die Unterschiede zur geltenden Rechtslage hervor.

2. Begriff und Anwendungsbereich

2.1. Begriff der Videoüberwachung

Videoüberwachung wird in § 50a Abs. 1 DSG als «die systematische, insbesondere fortlaufende Feststellung von Ereignissen, die ein bestimmtes Objekt (überwachtes Objekt) oder eine bestimmte Person (überwachte Person) betreffen, durch technische Bildaufnahme- oder Bildübertragungsgeräte» definiert. Von dieser Be-

¹ Dieser Beitrag gibt ausschließlich die persönliche Meinung des Autors wieder.

² Vgl. Art. 99 Abs. 1 DS-GVO.

³ Vgl. Art. 99 Abs. 2 DS-GVO.

⁴ So auch für Deutschland etwa FREIHERR VON DEM BUSSCHE/ZEITER/BROMBACH, Die Umsetzung der Vorgaben der EU-Datenschutz-Grundverordnung durch Unternehmen, Der Betrieb 2016, S. 1359.

⁵ Eine detaillierte Abhandlung würde den Rahmen dieses Beitrags sprengen.

griffsbestimmung sind nur Videoüberwachungen erfasst, die einem Kontrollzweck dienen.⁶ Jedoch fällt auch «gezieltes Fotografieren» mit Überwachungszweck unter den Begriff der Videoüberwachung nach § 50a Abs. 1 DSGVO.⁷ Für Videoüberwachungstätigkeiten, die nicht unter die Definition des § 50a Abs. 1 DSGVO fallen, gelten die allgemeinen Regelungen des DSGVO.

Die DS-GVO erwähnt den Begriff der «Videoüberwachung» zwar nicht ausdrücklich, stellt aber in ErwGr 91 zur DS-GVO auf «opto-elektronische Vorrichtungen» (also elektronische Videoüberwachung⁸) ab. Somit ist auch ausdrücklich klargestellt, dass Videoüberwachungstätigkeiten vom Begriff der «Verarbeitung» i.S.d. Art. 4 Z. 2 DS-GVO erfasst sind. Videoüberwachungstätigkeiten unterfallen den Regelungen der DS-GVO, wenn dabei personenbezogene Daten⁹ verarbeitet werden. Unter Videoüberwachungstätigkeiten wird im Folgenden die Beobachtung von Orten und/oder Personen durch optisch-elektronische Vorrichtungen (Digitalkameras, Videokameras, etc.) verstanden.

2.2. Räumlicher Anwendungsbereich der DS-GVO bei Videoüberwachung

Ist der Verantwortliche (oder auch der Auftragsverarbeiter) in der Union oder an einem Ort, der aufgrund Völkerrechts dem Recht eines Mitgliedstaats unterliegt¹⁰, niedergelassen, so ist die DS-GVO auf Videoüberwachungstätigkeiten anwendbar, unabhängig davon, ob die Verarbeitung tatsächlich in der Union stattfindet oder nicht.¹¹ Daneben ist die DS-GVO auch anwendbar, wenn personenbezogene Daten im Rahmen der Videoüberwachungstätigkeit von nicht in der Union befindlichen Niederlassungen von Verantwortlichen oder Auftragsverarbeitern verarbeitet werden, sofern die Datenverarbeitung im Zusammenhang damit steht, das Verhalten betroffener Personen zu beobachten, soweit ihr Verhalten in der Union erfolgt.¹²

2.3. Videoüberwachung zu privaten Zwecken

Ob Videoüberwachung zu privaten Zwecken vom Begriffsumfang der Videoüberwachung in § 50a Abs. 1 DSGVO erfasst ist, ist umstritten.¹³ Die DS-GVO ist für Verarbeitungen personenbezogener Daten im Rahmen von Videoüberwachungstätigkeiten jedenfalls nicht anwendbar, sofern die Tätigkeit von einer natürlichen Person zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten¹⁴ und somit ohne Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit¹⁵ vorgenommen wird.

2.4. Erdbeobachtung mittels Satelliten

Die Verarbeitung personenbezogener Daten durch Erdbeobachtung mittels Satelliten unterfällt der DS-GVO, wenn (i) der gegenständliche Satellit im Einklang mit weltraumrechtlichen Regelungen der Jurisdiktion und

⁶ THIELE, Aktuelles zur Videoüberwachung – Erste Erfahrungen nach der DSGVO Novelle 2010, Teil 2, *jusIT* 2011, S. 14 (S. 15 f.).

⁷ LVwG Kärnten 7. Mai 2014, KLVwg-807-808/11/2014.

⁸ So auch FEILER/FORGÓ, EU-DSGVO (2016), Art. 35 Rz. 9.

⁹ Zu diesem Begriff siehe FRITZ, Anwendungsbereich und Rechtfertigung – Alles neu macht die DS-GVO? In: Jahnelt (Hrsg.), *Jahrbuch Datenschutzrecht* 2016, S. 9 (S. 11 ff.).

¹⁰ Dazu im Detail FRITZ, Anwendungsbereich und Rechtfertigung – Alles neu macht die DS-GVO? In: Jahnelt (Hrsg.), *Jahrbuch Datenschutzrecht* 2016, S. 9 (S. 25).

¹¹ Vgl. Art. 4 Abs. 1 und 3 DS-GVO.

¹² Vgl. Art. 4 Abs. 2 lit. b DS-GVO.

¹³ Dafür etwa HATTENBERGER, Die Bestimmungen des DSGVO zur Videoüberwachung – Hat sich der Aufwand gelohnt? In: Jahnelt, *Jahrbuch Datenschutzrecht* 2011, S. 117 (S. 123); dagegen etwa THIELE, Videoüberwachung aus Fahrzeugen – Datenschutzrechtliches zu Dashcams. In: Jahnelt (Hrsg.), *Jahrbuch Datenschutzrecht* 2014, S. 235 (S. 243).

¹⁴ Vgl. Art. 2 Abs. 2 lit. c DS-GVO.

¹⁵ Vgl. ErwGr 18 Satz 1 zur DS-GVO.

Kontrolle eines Mitgliedsstaates unterstellt¹⁶ ist¹⁷ oder (ii) die satellitengestützte Erdbeobachtung im Zusammenhang damit steht, das Verhalten von Personen in der Union zu beobachten.¹⁸

3. Zweckgebundenheit und Speicherdauer

3.1. Legitime Zwecke

Videoüberwachungen i.S.d. § 50a Abs. 1 DSGVO dürfen nur zu zwei bestimmten Zwecken betrieben werden, nämlich (i) der Schutz des überwachten Objekts oder der überwachten Person oder (ii) die Erfüllung rechtlicher Sorgfaltspflichten.¹⁹ Diese Zweck-Einschränkung fällt mit der DS-GVO weg. Gemäß der allgemeinen Regelung in Art. 5 Abs. 1 lit. b DS-GVO kann die Verarbeitung personenbezogener Daten im Rahmen von Videoüberwachungstätigkeiten auf jeden legitimen Zweck²⁰ gestützt werden.

3.2. Zufallstreffer

Regelte bisher § 50a Abs. 6 DSGVO den Umgang mit Zufallstreffern (also Aufzeichnungen, die im Rahmen einer Videoüberwachung gewonnen wurden, aber außerhalb des zulässigen Zwecks liegen²¹), so richtet sich der datenschutzkonforme Umgang mit Zufallstreffern unter der DS-GVO vollständig nach den allgemeinen Regelungen. Somit ist die beabsichtigte Verarbeitung eines Zufallstreffers entweder auf einen gesonderten datenschutzrechtlichen Rechtfertigungsgrund zu stützen oder nach dem «Kompatibilitätstest»²² gemäß Art. 6 Abs. 4 DS-GVO zu beurteilen. Enthält der Zufallstreffer strafrechtlich relevante Daten²³, so richtet sich die Zulässigkeit von deren Verarbeitung zumeist nach mitgliedstaatlichen Regelungen.²⁴

3.3. Datenabgleich und Durchsuchbarkeit

Nach § 50a Abs. 7 DSGVO dürfen mit einer Videoüberwachung i.S.d. § 50a Abs. 1 DSGVO gewonnene Daten von Betroffenen nicht automationsunterstützt mit anderen Bilddaten abgeglichen und nicht nach sensiblen Daten als Auswahlkriterium durchsucht werden. Mangels einschlägiger Sonderregelungen in der DS-GVO richten sich auch diese Vorgänge in Zukunft nach den allgemeinen Regelungen und sind daher zulässig, wenn sie auf einen gesonderten datenschutzrechtlichen Rechtfertigungsgrund gestützt werden können oder den «Kompatibilitätstest» gemäß Art. 6 Abs. 4 DS-GVO bestehen.

4. Datenschutzrechtliche Rechtfertigung

§ 50a Abs. 3 und 4 DSGVO beschränkten die Zulässigkeit einer Videoüberwachung auf wenige Rechtfertigungsgründe. Nach der DS-GVO wird die gesamte Bandbreite der zur Verfügung stehenden Rechtfertigungsgründe zur Begründung der Zulässigkeit herangezogen werden können. Hierfür ist insbesondere maßgeblich, ob es sich bei Bilddaten um (normale) personenbezogene Daten oder sensible Daten²⁵ handelt. Dies ist umstritten, auch im Hinblick auf die DS-GVO.²⁶

¹⁶ Dazu im Detail FRITZ, Der «lauching state» im Kontext privater Weltraumaktivitäten (2016) Rz. 181 ff.

¹⁷ Dann ist Art. 4 Abs. 3 DS-GVO erfüllt.

¹⁸ Dann ist Art. 4 Abs. 2 lit. b DS-GVO erfüllt.

¹⁹ Vgl. § 50a Abs. 2 DSGVO.

²⁰ Dazu etwa FEILER/FORGÓ, EU-DSGVO (2016), Art. 5 Rz. 6.

²¹ GERHARTL, Gesetzliche Regelung der Videoüberwachung, jusIT 2010, S. 104 (S. 106).

²² So SCHANTZ, Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht, NJW 2016, S. 1841 (S. 1844).

²³ Zu diesem Begriff nach der DS-GVO siehe FRITZ, Anwendungsbereich und Rechtfertigung – Alles neu macht die DS-GVO? In: Jahnel (Hrsg.), Jahrbuch Datenschutzrecht 2016, S. 9 (S. 16).

²⁴ Vgl. Art. 10 DS-GVO.

²⁵ Zu diesem Begriff nach der DS-GVO siehe FRITZ, Anwendungsbereich und Rechtfertigung – Alles neu macht die DS-GVO? In: Jahnel (Hrsg.), Jahrbuch Datenschutzrecht 2016, S. 9 (S. 13 ff.).

²⁶ Vgl. etwa KNYRIM, Bilddaten: immer sensibel?, jusIT 2016, S. 235 (S. 239 f.); BERGAUER, Die Einordnung von Bilddaten erkennbarer Personen im Datenschutzrecht, jusIT 2016, S. 241 (S. 244 ff.).

In ErwGr 51 Satz 3 zur DS-GVO wird ausdrücklich klargestellt, dass die Verarbeitung von Lichtbildern grundsätzlich nicht als Verarbeitung besonderer Kategorien von personenbezogenen Daten angesehen werden sollte, da (so die Begründung) Lichtbilder nur dann von der Definition des Begriffs «biometrische Daten» erfasst werden, wenn sie mit speziellen technischen Mitteln verarbeitet werden, die die eindeutige Identifizierung oder Authentifizierung einer natürlichen Person ermöglichen. Somit ist die Verarbeitung von Lichtbildern ohne Hinzutreten weiterer Elemente auch nicht als Verarbeitung personenbezogener Daten anzusehen, aus denen die rassische oder ethnische Herkunft oder der Gesundheitszustand einer Person hervorgeht (was auf Fotos oder Videos im Einzelfall durchaus erkennbar wäre).²⁷ Der einleitende Satzteil «Die Verarbeitung von Lichtbildern sollte nicht grundsätzlich als Verarbeitung besonderer Kategorien von personenbezogenen Daten angesehen werden» in ErwGr 51 Satz 3 wäre nämlich ansonsten sinnentleert, wenn nach der DSGVO Lichtbilder mit der Begründung, aus ihnen wäre immer die ethnische und/oder rassische Herkunft ablesbar, dann doch generell als besondere Kategorien von Daten (sensible Daten) anzusehen wären. Die Wendung «grundsätzlich nicht» deutet zudem darauf hin, dass hier ein weiteres Element hinzutreten muss, um Lichtbilder als «besondere Kategorien von Daten» nach der DSGVO qualifizieren zu können. Dieses zusätzliche Element kann – analog zu den im begründenden Satzteil erwähnten biometrischen Daten – insbesondere der Zweck der Datenverarbeitung sein. Wäre die Intention des Verordnungsgesetzgebers gewesen, mit ErwGr 51 Satz 3 lediglich auszudrücken, dass Lichtbilder nicht immer als biometrische Daten anzusehen seien, dann hätte dieser Satz m.E. anders formuliert sein müssen, etwa wie folgt (Änderung hervorgehoben): «Die Verarbeitung von Lichtbildern sollte nicht grundsätzlich als Verarbeitung von *biometrischen* Daten angesehen werden, da Lichtbilder nur dann von der Definition des Begriffs «biometrische Daten» erfasst werden, wenn sie mit speziellen technischen Mitteln verarbeitet werden, die die eindeutige Identifizierung oder Authentifizierung einer natürlichen Person ermöglichen». Auch der vorhergehende Satz (ErwGr 51 Satz 2 zur DS-GVO), welcher Daten über die rassische oder ethnische Herkunft zum Thema hat, dient als weiterer Anhaltspunkt dafür, dass sich der Verordnungsgesetzgeber der Thematik bewusst war, sich aber aktiv dagegen entschieden hat, ohne Hinzutreten weiterer Elemente (wie etwa ein bestimmter auf die Verarbeitung besonderer Kategorien von Daten abstellender Zweck der Datenverarbeitung) bei Lichtbildern vom Vorliegen besonderer Kategorien von Daten auszugehen, auch wenn aus diesen die ethnische und/oder rassische Herkunft der darauf abgebildeten Personen erkennbar wäre.

Zusammenfassend sind Bilddaten daher nicht immer als sensible Daten anzusehen, sondern nur bei Hinzutreten weiterer Elemente (wie etwa ein bestimmter auf die Verarbeitung sensibler Daten abstellender Zweck der Datenverarbeitung). Dies ist auch sachgerecht, da ansonsten in der Praxis die Verarbeitung personenbezogener Daten im Rahmen von Videoüberwachungstätigkeiten regelmäßig nur auf die vorherige ausdrückliche Einwilligung aller (!) betroffenen Personen gestützt werden könnte. Der Rechtfertigungsgrund des berechtigten Interesses²⁸ steht bei sensiblen Daten nämlich nicht zur Verfügung, womit bei Bejahung des generellen Vorliegens von sensiblen Daten eine Videoüberwachung ohne vorherige Einwilligung aller betroffenen Personen auch nicht zum Eigentumsschutz oder Objektschutz betrieben werden dürfte und eine dennoch zu diesem Zweck betriebene Videoüberwachungsanlage mit enormen Sanktionen²⁹ bedroht wäre.

²⁷ So bereits FRITZ, Anwendungsbereich und Rechtfertigung – Alles neu macht die DS-GVO? In: Jähnel (Hrsg.), Jahrbuch Datenschutzrecht 2016, S. 9 (S. 14 f.).

²⁸ Zu beachten ist, dass die DS-GVO im Gegensatz zur bisherigen Rechtslage, die ein *überwiegendes* berechtigtes Interesse verlangt, bereits genügen lässt, dass die Interessen der betroffenen Person nicht überwiegen; siehe FRITZ, Anwendungsbereich und Rechtfertigung – Alles neu macht die DS-GVO? In: Jähnel (Hrsg.), Jahrbuch Datenschutzrecht 2016, S. 9 (S. 29 m.w.N.).

²⁹ Vgl. Art. 83 DS-GVO.

5. Betroffenenrechte

5.1. Informationspflicht

Im Rahmen der nach der DS-GVO den Verantwortlichen treffenden Informationspflichten stellt sich die Frage, ob die Daten bei der betroffenen Person «erhoben» werden oder nicht. Je nachdem richtet sich die Verpflichtung entweder nach Art. 13 DS-GVO oder Art. 14 DS-GVO. Eine Datenerhebung bei der betroffenen Person sollte richtigerweise nur in Fällen bejaht werden, in denen die betroffene Person tatsächlich Kenntnis von den einzelnen erhobenen Daten hat, insbesondere weil sie diese (etwa durch Eingabe) selbst zur Verfügung gestellt hat.³⁰ Für die Verarbeitung personenbezogener Daten im Rahmen von Videoüberwachungstätigkeiten ist somit die Informationsverpflichtung nach Art. 14 DS-GVO zu beachten. Dies bedeutet eine signifikante Änderung zur bisherigen Rechtslage, die in § 50d DSG eine bloße Kennzeichnungspflicht vorsieht. Es ist wohl schwer vorstellbar, wie die Informationspflicht nach Art. 14 DS-GVO mit einem Piktogramm³¹ erfüllt werden könnte.

5.2. Auskunftsrecht

Wenngleich beim Auskunftsanspruch der betroffenen Person in der DS-GVO keine Sonderregel mehr besteht, fallen die inhaltlichen Änderungen gering aus.

5.2.1. Mitwirkungspflicht des Auskunftswerbers

§ 50e Abs. 1 DSG verlangt vom Auskunftswerber, sowohl den Zeitraum, in dem er möglicherweise von der Überwachung betroffen war, als auch den Ort möglichst genau zu benennen. Eine derartig detaillierte Mitwirkungspflicht ist beim Auskunftsrecht nach Art. 15 DS-GVO zwar nicht gefordert. Da bei Betrieb einer Videoüberwachungsanlage regelmäßig jedoch eine Identifizierung der betroffenen Personen nicht erforderlich ist, entfällt der Auskunftsanspruch, wenn der Verantwortliche nachweisen kann, dass er nicht in der Lage ist, den Auskunftswerber zu identifizieren, und dieser auch nicht zur Ausübung des Auskunftsrechts zusätzliche Informationen bereitstellt, die seine Identifizierung ermöglichen.³² Welche Informationen der Auskunftswerber beibringen muss, ist in der DS-GVO nicht abschließend geregelt. Es ist aber zu erwarten, dass die möglichst genaue³³ Angabe des Zeitraums, in dem er möglicherweise von der Überwachung betroffen war, als auch des Ortes (in Verbindung mit der Vorlage eines Lichtbildausweises) im Regelfall wohl ausreichen dürfte, um den Auskunftswerber zu identifizieren und eine Auskunft zu ermöglichen.

5.2.2. Form der Auskunft

Nach § 50e Abs. 1 DSG hat der Betroffene grundsätzlich einen Anspruch auf Erhalt einer Kopie der zu seiner Person verarbeiteten Daten in einem üblichen Format. Auch nach Art. 15 Abs. 3 DS-GVO ist der betroffenen Person eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung zu stellen. Wenngleich nur bei elektronischer Stellung des Auskunftsersuchens die Zurverfügungstellung in einem «gängigen elektronischen Format» verpflichtend vorgesehen sein, wird in der Praxis wohl auch bei nicht-elektronisch gestellten Auskunftsersuchen eine Zurverfügungstellung regelmäßig in einem gängigen elektronischen Format erfolgen, da eine andere Form der Zurverfügungstellung für den Verantwortlichen wohl regelmäßig (noch) aufwändiger wäre.³⁴

³⁰ So mit überzeugender Begründung FEILER/FORGÓ, EU-DSGVO (2016), Art. 13 Rz. 2.

³¹ Nach geltender Rechtslage wäre dies ausreichend; siehe DOHR/POLLIRER/WEISS/KNYRIM, DSG², § 50d Anm. 1.

³² Vgl. Art. 11 DS-GVO; weiters auch ErwGr 63 Satz 7 zur DS-GVO.

³³ Inwieweit die nach geltendem Recht bestehenden «Ungenauigkeitsgrenzen» auch unter der DS-GVO Bestand haben werden, kann im Rahmen dieses Beitrags nicht geklärt werden.

³⁴ Auf einem anderen Blatt steht natürlich, wer die Kosten der elektronischen Zurverfügungstellung tragen sollte, wenn die betroffene Person keine elektronische Kontaktierungsmöglichkeit angibt.

Gemäß Art. 15 Abs. 4 DS-GVO darf das Recht auf Erhalt der Kopie – wie schon im DSGVO³⁵ – die Rechte und Freiheiten anderer Personen nicht beeinträchtigen. Ob hier anstelle einer Unkenntlichmachung dritter Personen auch eine bloße Beschreibung des im Rahmen der Videoüberwachung verarbeiteten Verhaltens in Betracht kommt, mag wohl auch vor dem Hintergrund des Art 15 DS-GVO durchaus vertretbar sein. Zu beachten ist jedoch, dass hier auch eine gesetzgeberische Klarstellung auf nationaler Ebene möglich wäre.³⁶

5.3. Recht auf Berichtigung, Löschung und Datenübertragbarkeit

Ein Recht auf Berichtigung scheidet bei Videoüberwachungstätigkeiten aus, da a priori nicht erkennbar ist, wie die aufgezeichneten Daten einer bestimmten Person einer Berichtigung zugänglich sein sollten.

Das Recht auf Löschung wird in der Praxis wohl mit Unkenntlichmachung des Auskunftswerbers oder Löschung der entsprechenden Aufnahme umgesetzt werden müssen. Selbiges wird auch beim erfolgreich durchgesetzten Widerspruchsrecht gelten.

Die Durchsetzbarkeit des Rechts auf Datenübertragbarkeit scheidet daran, dass die Daten nicht von der betroffenen Person bereitgestellt, also «willentlich und wissentlich übermittelt»³⁷ wurden.

6. Zulässige Speicherdauer

Nach § 50b Abs. 2 DSGVO sind aufgezeichnete Daten im Regelfall nach spätestens 72 Stunden zu löschen. Nach der DS-GVO ist keine derartige Lösungsverpflichtung vorgesehen. Allerdings dürfen personenbezogene Daten nur solange in einer Form gespeichert werden, die die Identifizierung der betroffenen Person ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist.³⁸ Dies gibt daher Verantwortlichen zwar eine größere Flexibilität bei der Festlegung der Speicherdauer, diese sind allerdings für die (korrekte) Einhaltung dieses Grundsatzes verantwortlich und müssen dessen Einhaltung im Rahmen der sie treffenden Rechenschaftspflicht nachweisen können.³⁹

7. Wegfall der Meldepflicht / Verzeichnis von Verarbeitungstätigkeiten

Da die DS-GVO keine Meldepflicht mehr vorsieht, hat § 50c DSGVO in der DS-GVO keine Entsprechung. Anstelle der Meldepflicht tritt die Führung eines Verzeichnisses von Verarbeitungstätigkeiten, sofern der Verantwortliche nicht gemäß Art. 30 Abs. 5 DS-GVO davon ausgenommen ist.

8. Datenschutz-Folgenabschätzung

Ob bei einer Verarbeitung personenbezogener Daten im Rahmen von Videoüberwachungstätigkeiten eine Datenschutz-Folgenabschätzung erforderlich ist, ist einzelfallbezogen, insbesondere anhand der technischen Ausgestaltung und des Verarbeitungszwecks, zu beurteilen und insbesondere dann zu bejahen, wenn die Videoüberwachungstätigkeit eine «umfangreiche Verarbeitung» sensibler Daten oder strafrechtlich relevanter Daten beinhaltet.

9. Fazit

Durch den Wegfall der Sonderbestimmungen zur Videoüberwachung und der Anwendbarkeit allgemeiner Bestimmungen der DS-GVO auf die Verarbeitung personenbezogener Daten im Rahmen von Videoüberwachungstätigkeiten kommt es in einigen Bereichen zu Änderungen der anwendbaren datenschutzrechtlichen Bestimmungen. Insbesondere die Qualifikation von Bilddaten als sensible Daten würde die Zulässigkeit von Videoüberwachungstätigkeiten massiv beschränken.

³⁵ Vgl. § 50e Abs. 2 DSGVO.

³⁶ Vgl. Art. 23 Abs. 1 lit. i DS-GVO.

³⁷ So FEILER/FORGÓ, EU-DSGVO (2016), Art. 20 Rz. 4.

³⁸ Vgl. Art. 5 Abs. 1 lit. e DS-GVO.

³⁹ Vgl. Art. 5 Abs. 2 DS-GVO.