09 2019

525 – 592

ÖSTERREICHISCHES Anwalts blatt

www.rechtsanwaelte.at

MANZ

Österreichische Post AG · MZ 02Z032542 M · Österreichischer Rechtsanwaltskammertag, Wollzeile 1 – 3, 1010 Wien · ISSN 1605-2544

Abhandlungen

CHRISTIAN ZEILINGER
Der Autor ist selbstständiger Rechtsanwalt in Oberösterreich mit den Schwerpunkten Datenschutzrecht, dabei insbesondere der DSGVO, sowie IT-Recht, Internet-, AGB- und Vertragsrecht.

ANDREA WÜNSCHER
Die Autorin ist juristische Mitarbeiterin der Kanzlei.

2019/223

Datenschutzrechtliche Schranken von Videoaufnahmen

Anhand ausgewählter Beispiele und Entscheidungen wird die Zulässigkeit von Videoaufnahmen in unterschiedlichen Bereichen erörtert. Vor allem im Hinblick auf die DSGVO soll ein Überblick über aktuelle Entwicklungen im Datenschutzrecht in Bezug auf Videoaufnahmen geboten werden.

I. ZULÄSSIGKEIT VON VIDEOAUFNAHMEN ANHAND AUSGEWÄHLTER BEISPIELE

1. Überwachung der eigenen Liegenschaft durch Videokameras bzw Kamera-Attrappen

Private Videoaufnahmen, die nur das eigene Grundstück bzw Gebäude zeigen, sind grundsätzlich zulässig, solange sie nicht den öffentlichen Bereich oder Teile davon (zB Gehsteige oder Straßen) miterfassen. Gem Art 2 Abs 2 lit c DSGVO sind darüber hinaus alle rein familiären Tätigkeiten, selbst wenn damit auch personenbezogene Daten verarbeitet werden, ausgenommen (sog „Haushaltsausnahme").[1]

Das DSG erlaubt Bildaufnahmen gem § 12 Abs 3 Z 1 insb dann, wenn „sie dem vorbeugenden Schutz von Personen oder Sachen auf privaten Liegenschaften, die ausschließlich vom Verantwortlichen genutzt werden, dient, und räumlich nicht über die Liegenschaft hinausreicht, mit Ausnahme einer zur Zweckerreichung allenfalls unvermeidbaren Einbeziehung öffentlicher Verkehrsflächen". Es muss für den Aufnehmenden zusätzlich ein „überwiegend berechtigtes Interesse" vorliegen und die Verhältnismäßigkeit gewahrt werden. Mit Videoaufnahmen verbundene Tonaufnahmen sind im Einzelfall zu beurteilen und in den Fällen des § 12 Abs 3 Z 1 und 2 DSG wohl nicht zulässig.[2]

Kamera-Attrappen, die keine tatsächlichen Bilder aufnehmen können, fallen weder unter den Anwendungsbereich des DSG noch der DSGVO.[3] Dasselbe gilt für Kameras, die zwar an sich echt, aber nicht funktionstüchtig sind.[4] Allerdings können Kamera-Attrappen, die den Eindruck einer Überwachung schaffen, aus dem Grund der Beeinträchtigung der Privatsphäre unzulässig sein.[5]

2. Digitale Türspione

Die Anwendung digitaler Türspione, die häufig bei Wohnungstüren in Mehrparteienhäusern eingesetzt werden, kann unter Umständen unzulässig sein.[6] Beim Betrieb eines solchen Türspions handelt es sich um eine Bildaufnahme iSd § 12 Abs 1 DSG, da eine technische Einrichtung vorliegt, die darauf gerichtet ist festzustellen, welche Personen sich wann im Aufnahmebereich befinden. Diese Erfassung lässt sich unter eine Datenverarbeitung iSd Art 4 Z 2 DSGVO subsumieren. Problematisch bei der Verwendung der digitalen Türspione ist hierbei vor allem, dass sie meistens den höchstpersönlichen Lebensbereich betroffener Personen, also etwa Nachbarn oder Besucher, miterfassen. Auch das Verlassen oder Betreten der Wohnung zählt iSd § 12 Abs 4 Z 1 DSG hierzu. Demnach ist die Aufnahme des höchstpersönlichen Lebensbereichs, der als Kernbereich der geschützten Privatsphäre etwa auch das Sexualleben, das allgemeine Familienleben oder die Gesundheitssphäre umfasst,[7] nur nach Zustimmung der betroffenen Person zulässig. Denkbar ist es, eine Zustimmung von sämtlichen Nachbarn vor Installation eines digitalen Türspions einzuholen. Trotzdem kann es sich um eine unzulässige Verarbeitung handeln, sobald zB Besucher ohne vorherige Einwilligung aufgenommen werden.

3. Drohnen

Werden bei Drohnen, also unbemannten Flugobjekten, die mit einem Bildaufnahmegerät ausgestattet sind, personenbezogene Daten erfasst, liegt eine Verarbeitung vor, die unter das DSG und die DSGVO fällt. Damit gelten also auch hier die unter Pkt 1. bereits genannten Grundsätze: Ein öffentlicher Grund darf grundsätzlich nicht von der Aufnahme erfasst werden; aber auch die Aufnahme anderer Personen oder der Liegenschaft anderer Personen ist nicht zulässig, wenn kein berechtigtes Interesse daran besteht. Ein solches wird in den seltensten Fällen gegeben sein. Selbst Aufnahmen von Drohnen, die nicht gespeichert werden, sondern nur in Echtzeit übertragen werden, sind vom Anwendungsbereich des DSG und der DSGVO umfasst.[8] Liegen also nicht nur rein private Aufnahmen für familiäre Zwecke vor, sind Drohnenflüge mit einer Bildaufnahme aus datenschutzrechtlicher Sicht nur sehr beschränkt möglich. Eine rechtmäßige Aufnahme von Bildern und Videos

[1] *Jahnel,* Das Datenschutz-Anpassungsgesetz, in *Jahnel* (Hrsg), Datenschutzrecht. Jahrbuch 17 (2017) 275f.
[2] *Bresich/Dopplinger/Dörnhöfer/Kunnert/Riedl,* Datenschutzgesetz – Kommentar (2018) 134.
[3] *Schrems,* Private Videoüberwachung (2011) 27.
[4] Vgl DSK, K121.150/0014-DSK/2006.
[5] Vgl dazu etwa OGH 28. 3. 2007, 6 Ob 6/06k.
[6] Vgl Bescheid der Datenschutzbehörde DSB-D123.204/0005-DSB/2018.
[7] Vgl RIS-Justiz RS0122148.
[8] Vgl RV 472 BlgNR 24. GP 19. Es wird festgestellt, dass Echtzeitübertragungen Datenanwendungen darstellen. Zust auch *Schweiger,* Echtzeitaufnahmen – Datenschutz? https://www.dataprotect.at/2019/06/02/echtzeitaufnahmen-datenschutz/ (abgefragt am 8. 6. 2019).

mittels Drohnen kann nur dann gegeben sein, wenn es eine rechtliche Grundlage für die Verarbeitung gibt. Außer einem berechtigten Interesse ist bspw noch eine Einwilligung aller betroffenen Personen denkbar.

Zu beachten ist des Weiteren, dass der Verantwortliche für Betroffene nicht immer einfach zu erkennen ist und auch die in Art 12 ff DSGVO normierten Informationspflichten für eine Datenverarbeitung in der Regel nicht erfüllt werden können. Demnach sind Drohnenflüge inkl Bildaufnahmen über Wohngebieten, welche zB dem Zweck der Veröffentlichung im Internet dienen, nur selten als zulässig anzusehen.

Bei einer Nutzung von Drohnen werden künftig auch die Bestimmungen zu beachten sein, welche nach der neuen EU-Drohnenverordnung gelten.[9] Bspw müssen alle Drohnen, die mit einer Kamera ausgestattet sind, unabhängig von ihrem Gewicht, bei der österreichischen Gesellschaft für Zivilluftfahrt (Austro Control) registriert werden.

4. Dashcams

In Österreich ist die Aufnahme von Videos während des Autofahrens mittels sog „Dashcams", die der Beweissicherung bei Unfällen im Straßenverkehr dienen sollen, bereits nach dem Datenschutzgesetz aF unzulässig.[10] Auch nach Inkrafttreten der neuen Rechtslage im Datenschutz hat sich daran nichts geändert. Laut bisheriger Rsp seien die Aufnahmen aus dem Grund der Verhältnismäßigkeit als unzulässig anzusehen.[11] Vor allem im Hinblick auf die Zweckmäßigkeit der Beweissicherung bei Unfällen wäre nach Meinung der Verfasser ein Ausnahmetatbestand für Dashcams in Österreich wünschenswert – zumindest für solche Kameras, die keine permanente Überwachung des Straßenverkehrs inkl Datenspeicherung vornehmen, sondern lediglich bei einem drohenden Unfall automatisch speichern. Mittels Sensoren ist es möglich, dass Dashcams starkes Abbremsen oder Ausweichen erkennen und in einem solchen Fall eine Aufnahme abspeichern, die Daten während einer üblichen Fahrt aber ständig überschrieben werden. Das Interesse an den gesammelten Beweismitteln und eine daraus resultierende Möglichkeit zur Beschleunigung von Straf- und/oder Zivilprozessen, einhergehend mit einer Verbesserung im Hinblick auf die Verfahrensökonomie, überwiegt nach Meinung der Verfasser und sollte in diesem Fall den derzeitigen Regelungen des Datenschutzes, da ohnehin nur ein sehr geringer Eingriff vorliegen würde, vorgezogen werden. In anderen europäischen Ländern, wie bspw Großbritannien oder Italien, sind solche Aufnahmen bereits erlaubt und können auch vor Gericht als Beweismittel eingesetzt werden. In diesen Ländern wird der Einsatz von Dashcams von einigen Kfz-Versicherern etwa auch mit günstigeren Prämien honoriert.

Dashcam-Aufnahmen für rein familiäre Zwecke, also etwa als Urlaubserinnerungen, die nicht veröffentlicht werden, verstoßen nicht gegen datenschutzrechtliche Vorschriften, selbst wenn personenbezogene Daten aufgenommen werden. Dies ergibt sich einerseits aus der bereits erwähnten „Haushaltsausnahme" des Art 2 Abs 2 lit c DSGVO wie auch aus § 12 Abs 3 Z 3 DSG, der eine Zulässigkeit bestimmt, wenn die Bildaufnahme „ein privates Dokumentationsinteresse verfolgt, das nicht auf die identifizierende Erfassung unbeteiligter Personen oder die gezielte Erfassung von Objekten, die sich zur mittelbaren Identifizierung solcher Personen eignen, gerichtet ist". Im Einzelfall ergibt sich daraus natürlich das schwierige Beweisproblem des Zwecks der Videoaufnahmen.

5. Bodycams

Nach ersten Tests, die bis Ende Februar 2017 liefen, fiel die Entscheidung für Bodycams in regelmäßigen Polizeieinsätzen.[12] Die Bildaufnahmen sind zulässig, da keine ständige Aufzeichnung erfolgt, sondern erst nach manueller Betätigung und nach ausdrücklicher Ankündigung durch den jeweiligen Beamten aufgenommen wird.[13] Anders als in Deutschland, wo eine Speicherung der Aufnahmen auch trotz anhaltender Kritik von Datenschützern auf Servern des Konzerns „Amazon" erfolgt,[14] sollen die Daten in Österreich innerhalb interner Systeme sechs Monate lang gespeichert werden, was eine höhere Datensicherheit bedeuten kann.[15] Nach diesen sechs Monaten erfolgt eine Löschung, wenn die Aufnahmen nicht etwa in einem Strafprozess als Beweismittel Verwendung finden.

In Österreich sind nicht nur Polizisten mit Bodycams ausgestattet – bereits seit mehreren Jahren filmen zum Teil Mitarbeiter des Sicherheitsdienstes und Zugbegleiter der ÖBB ebenfalls mittels einer Kamera, die am Körper getragen wird. Aktiviert werden soll die Bodycam nur, wenn der Verdacht auf einen strafrechtlich relevanten Vorfall besteht.[16]

[9] Durchführungsverordnung (EU) 2019/947 der Kommission v 24. 5. 2019 über die Vorschriften und Verfahren für den Betrieb unbemannter Luftfahrzeuge https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32019R0947&from=EN (abgefragt am 14. 6. 2019).
[10] Vgl etwa Erk des VfGH v 12. 9. 2016, Ro 2015/04/0011.
[11] Entscheidung der Datenschutzbehörde mittels Bescheid v 9. 7. 2018, DSB-D485.000/0001-DSB/2018.
[12] Vgl *Lehmann*, Die Erprobung von Bodycams bei der Polizei. Unterschiede in den Vereinigten Staaten, Österreich und Deutschland, SIAK-Journal – Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis 2017, 31.
[13] Vgl BMI-LR2220/0205-II/2/b/2019–2999/AB 26. GP – Anfragebeantwortung Bundesminister Herbert Kickl vom 29. 4. 2019.
[14] Vgl schriftliche Frage des Abgeordneten zum Deutschen Bundestag Benjamin Strasser v 21. 2. 2019 https://www.benjamin-strasser.de/files/Bilder%20und%20Dateien/Bilder%20Aktuelles/aktuelles_2/Einzelfrage_Bodycams_Amazon.pdf (abgefragt am 08. 6. 2019).
[15] Im Hinblick auf die fehlende Zulässigkeit von Dashcams (s Pkt 3.), die im Grunde demselben Zweck dienen (Beweissicherung für Prozesse), ist allerdings eine unterschiedliche Behandlung der beiden Aufnahmemöglichkeiten zu kritisieren. Der wohl einzige Unterschied besteht in der Vorankündigung von Bodycam-Aufnahmen, da eine solche bei Dashcams nicht erfolgt.
[16] Vgl Presseinformation ÖBB: Auch Zugbegleiter werden mit BodyCams ausgestattet vom 2. 5. 2017, https://presse.oebb.at/de/presseinformationen/oebb-auch-zugbegleiter-werden-mit-bodycams-ausgestattet (abgefragt am 14. 6. 2019).

6. Mitarbeiterüberwachung

Für die Zulässigkeit von Videoaufnahmen, auf denen Mitarbeiter zu sehen sind, wären die in den §§ 12 und 13 DSG geregelten Vorschriften zu beachten. In der DSGVO wird die Zulässigkeit von Videoaufzeichnungen dagegen nicht ausdrücklich geregelt. Eine Echtzeitüberwachung ohne Speicherung der Daten ist ebenfalls vom Anwendungsbereich der DSGVO umfasst.[17] § 12 Abs 4 Z 2 DSG normiert eine ausdrückliche Unzulässigkeit von Bildaufnahmen, die dem Zweck der Arbeitnehmerkontrolle dienen. Ebenso unzulässig sind nach Z 3 und 4 leg cit der automationsunterstützte Abgleich von mittels Bildaufnahmen gewonnenen personenbezogenen Daten ohne eine ausdrückliche Einwilligung oder eine Auswertung von mittels Bildaufnahmen gewonnenen personenbezogenen Daten anhand von besonderen Kategorien[18] personenbezogener Daten als Auswahlkriterium. Nach dem Wortlaut des § 12 DSG sind nunmehr lediglich Arbeitnehmer von der Kontrolle ausgeschlossen. § 50a Abs 5 DSG 2000 untersagte hingegen eine Videoüberwachung zum Zweck der Mitarbeiterkontrolle an Arbeitsstätten, weshalb vertreten wurde, dass auch freie Dienstnehmer davon erfasst sind.[19]

Die Reichweite des Verbots ist nicht eindeutig geklärt. Den Materialien der DSG-Novelle 2010 ist zu entnehmen, dass jegliche Leistungskontrolle mittels Videoaufnahmen verboten ist. Demnach ist es bspw nicht zulässig, dadurch eine Anwesenheitskontrolle durchzuführen; es soll also nicht die allgemeine Vertragserfüllung überwacht werden.[20] Besteht ein konkreter Verdacht einer strafbaren Handlung eines Mitarbeiters, könnte eine Videoüberwachung in Betracht gezogen werden, da in diesem Fall nicht auf die Überwachung der Vertragserfüllung abgezielt wird. Eine systematische Überwachung durch Kameras am Arbeitsplatz ist davon allerdings nicht mehr umfasst.[21]

Die Zulässigkeit der Überwachung bestimmter Objekte oder öffentlich zugänglicher Bereiche der Arbeitsstätte ist uU unter Berücksichtigung der Erlaubnistatbestände möglich. Solche sind in § 12 Abs 2 DSG normiert, wobei Z 4 leg cit eine Interessenabwägung fordert, nicht allerdings die Z 1 – 3.

Im Verzeichnis der Verarbeitungstätigkeiten muss die Tätigkeit „Bildverarbeitung" gem Art 30 DSGVO aufgenommen werden;[22] nach dem DSG ist jeder Verarbeitungsvorgang einzeln genauestens zu erfassen.

Nicht eindeutig geklärt ist allerdings, ob es sich bei den Aufnahmen um Daten einer besonderen Kategorie handelt. Dafür spricht bei Videodaten etwa die Möglichkeit einer Zuordnung des Mitarbeiters zu einer bestimmten Religion (zB beim Tragen eines Kopftuchs), was ein Datum besonderer Kategorie darstellt.[23] Geht man bei Videoaufnahmen von Daten einer besonderen Kategorie aus, müsste für jede Verarbeitung immer ein Rechtfertigungsgrund nach Art 9 Abs 2 DSGVO vorliegen. Richtigerweise ist wohl eine differenzierte Betrachtungsweise notwendig;[24] vor allem in Anbetracht der Tatsache, dass sich der EuGH in einer Entscheidung aus dem Jahr 2014[25] im Hinblick auf die Zulässigkeit der Datenverarbeitung auf nicht sensible Daten bezog. Weiters stellte er fest, dass die Rechtsgrundlage „Berechtigtes Interesse" für die Daten der Videoüberwachung als zulässig anzusehen ist, was für sensible Daten allerdings nicht möglich wäre.

Ist der Zweck für die Verarbeitung der personenbezogenen Daten nicht mehr gegeben und stehen auch keine anderen gesetzlichen Aufbewahrungspflichten entgegen, sieht das DSG wie auch die DSGVO eine Löschpflicht vor. Für eine länger als 72 Stunden dauernde Aufbewahrung, die immer verhältnismäßig sein muss, braucht es eine Protokollierung und Begründung. Zulässig wäre bspw eine Speicherung aus Beweissicherungsgründen.

[17] Anderer Ansicht *Grünanger* in *Grünanger/Goricnik* (Hrsg), Arbeitnehmer-Datenschutz und Mitarbeiterkontrolle[2] (2018) 213, der Echtzeitaufnahmen nicht unter den Anwendungsbereich der DSGVO subsumiert.
[18] Auch genannt „sensible Dateien".
[19] *Löschnigg,* Videoüberwachung iSd Entwurfs zur DSG-Novelle 2010 aus arbeitsrechtlicher Sicht, in *Bergauer,/Staudegger* (Hrsg), Recht und IT (2009) 63 f.
[20] ErläutRV 472 BlgNR 24. GP 19.
[21] *Grünanger* in *Grünanger/Goricnik* (Hrsg), Arbeitnehmer-Datenschutz und Mitarbeiterkontrolle[2] (2018) 220.
[22] *Hartung* in *Kühling/Buchner* (Hrsg), DS-GVO Kommentar Art 30 Rz 14 f.
[23] *Knyrim,* Bilddaten: immer sensibel? jusIT 2016/102, 235.
[24] Vgl etwa auch *Schweiger,* Fotos als sensible Daten? www.dataprotect.at/2018/04/27/fotos-als-senible-daten (abgefragt am 11. 4. 2018).
[25] EuGH 11. 12. 2014, C-212/13.

II. SONDERPROBLEME

1. Datenspeicherung in Clouds

Datenschutz und Cloudspeicherung sind kein grundsätzlicher Widerspruch. Dennoch könnte eine Speicherung der Videoaufnahmen in einer Cloud problematisch sein. Denn die DSGVO verlangt für die Verarbeitung von Daten, wozu zweifelsfrei auch eine Speicherung gehört, ein angemessenes Sicherheitsniveau auf dem Stand der Technik. Wie sich in der Vergangenheit bereits mehrmals gezeigt hat, können Cloudsysteme durch Hackerangriffe oftmals keine ausreichende Sicherheit der Daten gewährleisten oder die Daten werden gar unverschlüsselt gespeichert. Es gibt aber auch Anbieter, die ua durch eine Verschlüsselung aller Daten der DSGVO entsprechen und damit einer Nutzung zugänglich sind.

2. Datenverkehr mit Drittländern

Der Datenverkehr mit Drittländern ist nicht in jedem Fall zulässig. Eine Übermittlung in Länder des EWR sowie in die USA (solange der Empfänger dem EU-US-Privacy-Shield unterliegt) ist, vorausgesetzt die innerstaatliche Verarbeitung erfolgte DSGVO-konform, zulässig. Auch einige weitere Länder sind laut Angemessenheitsbeschluss der EU-Kommission als zulässig für den Datenverkehr zu sehen, da diese ein angemessenes Datenschutzniveau sicherstellen sollen. Dies sind bspw Neuseeland, Kanada oder Argentinien.

Sollen Videoaufnahmen daher auf Servern außerhalb dieser Länder gespeichert oder anderweitig verarbeitet werden, gilt es, die speziellen Informationspflichten des Verantwortlichen iSd DSGVO zu beachten und Standardvertragsklauseln zu vereinbaren. Des Weiteren gibt es die Möglichkeit, dass betroffene Personen einer Datenübermittlung in Drittländer, nach Information über mögliche Risiken, ausdrücklich zustimmen. Auf eine Zustimmung kann ua verzichtet werden, wenn die Übermittlung durch einen Vertrag gedeckt ist oder lebenswichtige Interessen der betroffenen Person dies erforderlich machen. Art 49 DSGVO nennt alle diesbezüglichen Ausnahmen.

III. AUSGEWÄHLTE ENTSCHEIDUNGEN

1. Datenschutzbehörde

a) DSB-D550.038/0003-DSB/2018 – Straferkenntnis

Das in Österreich erste rechtskräftige Straferkenntnis der Datenschutzbehörde nach Inkrafttreten der DSGVO erfolgte Ende 2018 aufgrund einer Videoüberwachung. Ein Wettlokalbetreiber installierte Videokameras einer Überwachungsanlage, mit der am Eingangsbereich auch eine Verkehrsfläche und somit Teile des öffentlich zugänglichen Bereichs miterfasst wurden. Des Weiteren fehlte auch eine ordnungsgemäße Kennzeichnung.

Der sachliche Anwendungsbereich des Art 2 DSGVO sei „durch das Erheben, Speichern und Übermitteln der gegenständlichen Bilddaten“ eröffnet. Auch stellen die Bilddaten zweifelsfrei personenbezogene Daten iSd Art 4 Z 1 DSGVO dar und das Wettbüro ist iSd Art 4 Z 7 DSGVO Verantwortlicher. Inhaltlich wurde festgestellt, dass durch die Bildaufnahmen des öffentlichen Raums, und damit unweigerlich auch vorbeikommender Verkehrsteilnehmer, gegen die Grundsätze des Art 5 DSGVO verstoßen wurde. Des Weiteren ist auch keine in Art 6 Abs 1 DSGVO normierte Rechtmäßigkeit der Verarbeitung einschlägig.

Auch gegen die Vorschrift des § 13 Abs 2 iVm § 62 Abs 1 Z 4 DSG verstieß der Betreiber des Wettbüros, da der Verarbeitungsvorgang weder protokolliert noch die aufgenommenen Daten rechtzeitig gelöscht wurden, wie es wiederum § 13 Abs 3 vorsieht.

Durch die fehlende Kennzeichnung der Videoüberwachung wurde zusätzlich der § 13 Abs 5 DSG verletzt.

2. OGH

a) 6 Ob 16/18y – Private Videoüberwachung eines Servitutswegs zur Gewinnung von Beweismitteln

Der OGH vertritt die Ansicht, dass die Videoüberwachung eines Servitutswegs zum Zweck der Gewinnung von Beweismitteln nach dem DSG 2000 nicht rechtmäßig ist, da dies unter keinen der gesetzmäßigen Gründe für einen Eingriff in das Geheimhaltungsinteresse des Betroffenen fällt und § 50a Abs 3 und 4 DSG die Beweissicherung für einen Zivilrechtsstreit nicht explizit nennt.

Dem Kläger wurde ein Servitutsrecht in Form eines Geh- und Fahrtrechts auf einem Weg des beklagten Nachbarn einverleibt. Aufgrund von mehrmaligem Abstellen von Fahrzeugen auf dem Weg und die dadurch nicht rechtmäßige Nutzung der Dienstbarkeit waren mehrere Zivilprozesse der beiden Parteien anhängig. Es erging auch ein Unterlassungsurteil, an welches sich die klagende Partei allerdings nicht hielt. Um diese Tatsache umfassend zu dokumentieren, installierte der Beklagte eine Videoüberwachungsanlage. Sekundär sollten die Aufnahmen auch zur Überwachung des Grundstücks und des Hauses vor unbefugtem Eindringen dienen. Die beiden Videokameras erfassten ausschließlich das Grundstück und Haus des Beklagten inklusive Zufahrtsweg. Der Kläger ist also darauf nur zu sehen, wenn der Servitutsweg – berechtigterweise oder unbefugt durch das Abstellen von Fahrzeugen – benutzt wird.

Der Kläger begehrte die Entfernung der Videokameras mit den Argumenten, dass diese einen massiven Eingriff in die Privatsphäre darstellen und auch die datenschutzrechtlichen Voraussetzungen nicht vorlägen. Die Gründe für die Installation seien nicht von den Ausnahmetatbeständen des Datenschutzgesetzes umfasst.

Allerdings hatte der OGH Bedenken bezüglich des allgemeinen Entfernungsbegehrens des Klägers und sprach sich daher für eine neuerliche Erörterung zur Formulierung des Begehrens aus. Der Revision wurde daher Folge gegeben

und die Rechtssache zur neuerlichen Verhandlung an das Erstgericht zurückverwiesen.

§ 50a DSG trat am 24. 5. 2018 allerdings außer Kraft, weshalb nun die Bestimmungen der §§ 12 und 13 DSG iVm der DSGVO zu beachten sind. Demnach ist eine Videoüberwachung zulässig, wenn ein überwiegendes berechtigtes Interesse und die Verhältnismäßigkeit gegeben sind. Da die Aufzählung des § 12 DSG, anders als § 50a DSG 2000, nicht taxativ ist (arg: „insbesondere"), könnte das fortgesetzte Verfahren in Hinblick auf die neuen Bestimmungen einen anderen Ausgang finden.[26]

b) 3 Ob 195/17y – Zulässigkeit einer Videoüberwachung bei Verpixelung der Daten

Trotz Verpixelung jener Bereiche, in denen die Videokamera auf das Nachbargrundstück zeigt, bleibt der Überwachungsdruck bestehen und die Aufzeichnung ist damit in diesem Fall rechtswidrig.

Der Kläger begehrte ein Zivilverfahren bei der Datenschutzbehörde aufgrund einer Videokamera, die Teile dessen Liegenschaft zeige. Die Datenschutzbehörde stellte das Verfahren allerdings mit der Begründung ein, dass eine Überwachung ausschließlich für persönliche Zwecke erfolgte und das DSG bzw die DSGVO damit nicht anwendbar ist. Eine Überwachung im rein privaten Bereich ist mit Einschränkungen zulässig.

Daraufhin brachte der Kläger eine Klage mit Unterlassungsbegehren beim Erstgericht ein, da der Beklagte vier Videokameras installierte, die dessen Grundstück permanent überwachten. Bilder, die das Grundstück des Klägers zeigten, wurden nur in verpixelter Form übertragen. Des Weiteren erfolgte auch eine Löschung der aufgenommenen Bilder nach einem Ablauf von 72 Stunden.

Allerdings stellte der OGH fest, dass dennoch und trotz der Verpixelung das Persönlichkeitsrecht des Klägers beeinträchtigt und die Situation als „Überwachungsdruck" und damit als Eingriff in die Privatsphäre wahrgenommen wird, da von außen nicht ersichtlich ist, welche konkreten Bereiche die Kameras erfassen.

3. EuGH

a) C-345/17 – Videoaufzeichnung von Polizeibeamten in einer Dienststelle

Eine von einer Privatperson selbst erstellte und im Internet veröffentlichte Videoaufzeichnung von Polizeibeamten in ihrer Arbeitszeit fällt in den Anwendungsbereich der DSRL – damit auch der DSGVO.

Eine Privatperson filmte in Lettland seine Aussage in einer Polizeidienststelle, die auch die Beamten zeigte, und stellte diese Aufnahme auf eine Plattform für jeden öffentlich sichtbar ins Internet. Die lettische Datenschutzbehörde forderte die Person auf, das Video zu löschen, da sie als Verantwortliche gegen die Informationspflichten nach der DSRL verstieß, woraufhin der Verantwortliche Rechtsmittel einlegte.

Der EuGH stellte fest, dass es sich durch das Veröffentlichen auf der Plattform nicht um eine ausschließlich persönliche oder familiäre Tätigkeit handelte.

IV. STRAFBESTIMMUNGEN NACH DEM DSG UND DER DSGVO

Das DSG sieht bei Datenverwendung in Gewinn- und Schädigungsabsicht in § 63 eine strafrechtliche Bestimmung vor, deren Strafrahmen bis zu einem Jahr Freiheitsstrafe oder bis zu 720 Tagessätzen beträgt. Daneben enthält § 62 DSG eine Verwaltungsstrafbestimmung, die mit einer Geldstrafe von bis zu € 50.000,– zu ahnden ist.

Nach Wirksamwerden der DSGVO am 25. 5. 2018 liegt der Strafrahmen bei Verletzungen der Verordnung bei maximal 20 Mio Euro bzw bis zu 4% des weltweiten Konzernumsatzes des Vorjahres, je nachdem, welcher Betrag höher ist. Für geringfügigere Delikte ist allerdings die Hälfte davon vorgesehen. Diese Geldstrafen werden von der jeweiligen Datenschutzbehörde verhängt. Die Datenschutzbehörde soll bei Verstößen Geldbußen aussprechen, die wirksam, verhältnismäßig, aber auch abschreckend wirken. Dennoch wird beim ersten Verstoß häufig von der Möglichkeit einer Verwarnung Gebrauch gemacht.

Daneben bleibt das Recht auf Schadenersatz gegen den Verantwortlichen nach Art 82 DSGVO bestehen, wie § 28 DSG festlegt. Das Recht auf Geltendmachung von Schadenersatz hat jede Person, der bei einem Verstoß ein materieller oder immaterieller Schaden entstanden ist.

V. FAZIT

Abschließend kann festgehalten werden, dass in Österreich eine eher restriktive datenschutzrechtliche Zulässigkeit für Videoaufnahmen vorherrscht. Für rein private iSv familiären Aufnahmen liegt grundsätzlich ein Ausnahmetatbestand vor, selbst wenn personenbezogene Daten verarbeitet werden. Dieser gilt allerdings nicht für Aufnahmen des höchstpersönlichen Lebensbereichs einer betroffenen Person iSd § 12 Abs 4 Z 1 DSG. Solche Aufnahmen sind immer nur nach vorheriger Einwilligung der betroffenen Person zulässig. Besonderes Augenmerk sollte auf eine Speicherung der Videoaufnahmen in Cloudsystemen oder auf Servern in Drittländern gelegt werden, da dies nicht in allen Fällen zulässig ist. Grundsätzlich ist oftmals eine Einzelfallbetrachtung bei Anwendungen von Videokameras anzulegen, wohingegen Dashcams in Österreich nach derzeitigem Stand, mit Ausnahme der familiären Aufnahmen, niemals zulässig sind.

Auch wenn die Handhabung in Österreich bezüglich Dashcams überdacht werden sollte, sind ansonsten die strengen Regelungen und Neuerungen durch das DSG und die DSGVO zu begrüßen.

[26] Zust *Schweiger*, OGH: Videokamera zur Beweissicherung unzulässig, 22. 7. 2018 https://www.dataprotect.at/2018/07/22/ogh-videokamera-zur-beweissicherung-unzul%C3%A4ssig (abgefragt am 8. 6. 2019)