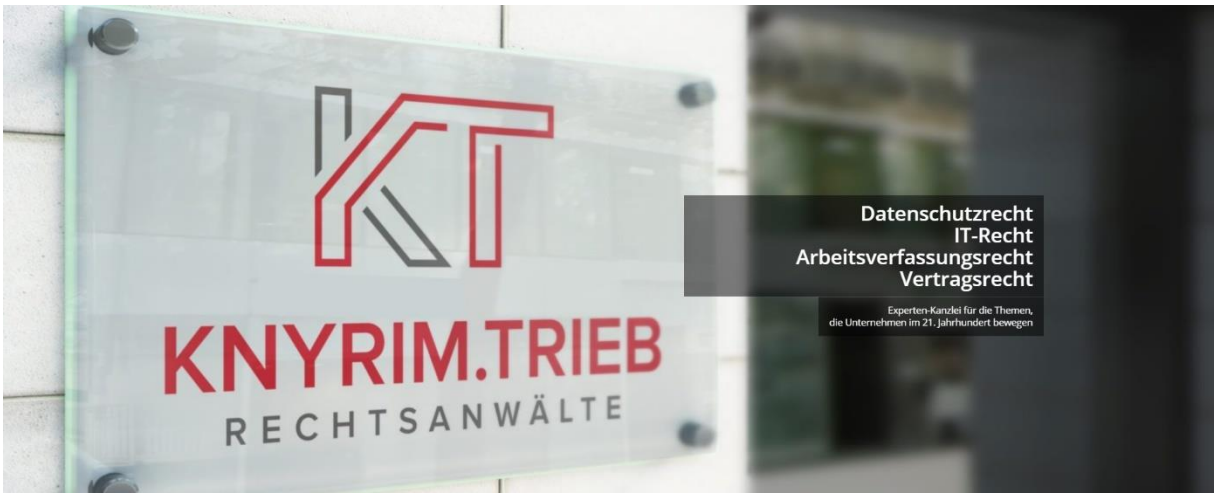

Newsletter 06.2020
Knyrim Trieb Rechtsanwälte OG

Sehr geehrte Damen und Herren!
Liebe Datenschutzinteressierte!

Im aktuellen Newsletter finden Sie einen Beitrag zum Thema Überwachung von Bürgern und Mitarbeitern und Informationen zu aktuellen Rechtsprechungen in Österreich im Bereich Videoüberwachung. Weiters gehen wir auf den vorgelegten Verordnungsentwurf für datenschutzrechtliche Zertifizierungen seitens der Datenschutzbehörde ein.

Datenschutz & Coronakrise:
Wie viel Überwachung von Bürgern und Mitarbeitern ist zulässig?

Beitrag erschienen 05.2020 im ecolex 2020 – Dr. Rainer Knyrim, Dr. Claudia Gabauer, LL.M. – KTR-Newsletter Juni 2020

Die COVID-19-Pandemie stellt den Datenschutz auf eine harte Probe.

Die COVID-19-Pandemie stellt den Datenschutz auf eine harte Probe. Die Nutzung moderner Technologien zu deren Bekämpfung ist Realität. Wie weit dürfen in der Krise Daten aus Mobiltelefonen über Bürger ausgewertet werden und in welchem Umfang darf der Arbeitgeber Gesundheitsdaten über seine Arbeitnehmer erheben?

Den Artikel finden Sie HIER

Quelle: https://rdb.manz.at/document/rdb.tso.LIecolex20200515

Videoüberwachung in Österreich:
Aktuelle Rechtsprechung

Beitrag verfasst von Mag. Andreas Rohner am 18.05.2020 – KTR-Newsletter Juni 2020

Der unrechtmäßige Betrieb von Bildverarbeitungssystemen bildet eine der häufigsten Grundlagen für die Verhängung von Geldbußen durch die österreichische Datenschutzbehörde. Über Beschwerden gegen diese Strafen entscheidet das Bundesverwaltungsgericht, das in den letzten Monaten einige beachtenswerte Entscheidungen zu dem Themenkreis der Bildverarbeitung veröffentlichte.

Anwendung nationaler Bestimmungen bei Bildverarbeitungen

In zwei kurz aufeinander folgenden Entscheidungen des Bundesverwaltungsgerichts und des Obersten Gerichtshofs kamen diese zu unterschiedlichen Ergebnissen hinsichtlich der Frage, ob die Vorgaben des österreichischen Datenschutzgesetzes (DSG) für die Bewertung der Zulässigkeit von Bildverarbeitungen vollumfänglich anwendbar sind oder nicht.

Bundesverwaltungsgericht (BVwG) [1]:
Die Besitzerin eines Kebab-Standes ließ mehrere Kameras installieren, nachdem er gemäß seinen Angaben regelmäßig Probleme mit einem schikanösen Polizisten gehabt habe. Eine der Kameras filmte bis zu einer nahegelegenen Tankstelle, es waren keine Hinweisschilder angebracht und die Aufzeichnungen wurden teils bis zu 16 Tage gespeichert. Die österreichische Datenschutzbehörde (DSB) verhängte in der Folge ein Bußgeld über den Besitzer des Kebab-Standes. Die Behörde wendete dabei die §§ 12 und 13 des DSG an, welche mehrere spezifische Auflagen für eine zulässige Bildverarbeitung vorsehen. Verletzt wurden in diesem Fall etwa die Kennzeichnungspflicht nach § 13 Abs 5 DSG und die Regelspeicherdauer von 72 Stunden gemäß § 13 Abs 3 DSG.

Das BVwG hielt demgegenüber im Beschwerdeverfahren (als auch in einem anderen Beschluss [2]) fest, dass mangels einer Öffnungsklausel in Art 6 Abs 1 DSGVO die von der DSB (und früher auch vom BVwG selbst) angewendeten Bestimmungen des DSG bei der Zulässigkeitsprüfung von Bildverarbeitungen nicht anwendbar sind.

Die österreichische Datenschutzbehörde (DSB) bestätigte diese Ansicht in der Folge und verlautbarte in ihrem Newsletter [3], die §§ 12 und 13 DSG bei der Beurteilung der Zulässigkeit von Bildverarbeitungen in der Regel nicht mehr anzuwenden, sondern ausschließlich auf Basis der Art 5 und 6 DSGVO prüfen.

Oberster Gerichtshof (OGH) [4]:

Nur zwei Tage nach der Entscheidung des BVwG, bewertete der OGH die Zulässigkeit einer vom Beklagten montierten Überwachungskamera an der Außenfassade seiner Wohnung, in deren Schwenkbereich auch ein allgemeiner Zugangsbereich fällt, neben Art 6 Abs 1 lit f DSGVO auch nach den §§ 12 und 13 DSG.

Vom OGH wurden diese Gesetzesstellen in der Prüfung herangezogen, da die §§ 12 und 13 DSG im Gegensatz zur DSGVO explizite Bestimmungen zur Bildverarbeitung enthalten. Im Endergebnis verlangte der OGH jedoch ebenfalls eine Verhältnismäßigkeitsprüfung für den Einzelfall. Im konkreten Fall überwogen die Interessen des Klägers auf Datenschutz und insbesondere seines Geheimhaltungsinteresses, weil die Kameraanlage des Beklagten einen öffentlichen Zugangsweg überwachte.

Fazit:
Der erhofften Rechtssicherheit im Zusammenhang mit der (Nicht)Anwendung der §§ 12 und 13 DSG schiebt der OGH mit seiner Entscheidung vorerst einen Riegel vor. Im Ergebnis sollte sich der Anwender dennoch auf die Art 5 und 6 DSGVO stützen, welche in jedem Fall für die Beurteilung der Zulässigkeit von Bildverarbeitungen vorrangig heranzuziehen sind. Bezüglich der zusätzlichen Anwendung der

Normen des DSG bleibt abzuwarten, welcher Ansicht die österreichischen Gerichte zukünftig folgen werden.

Zulässigkeit von Dashcams

Das BVwG widersprach in einem Erkenntnis vom 16.10.2019 [5] der Ansicht der DSB, dass der Einsatz von Dashcams durch Private im öffentlichen Bereich jedenfalls unzulässig sei. Vielmehr sei auch hier regelmäßig eine Einzelfallbetrachtung und eine Interessenabwägung vorzunehmen.

Sachverhalt:
Gegenstand des Verfahrens war die Kollision zweier KFZ, bei der es zu einer Beschädigung des Außenspiegels des Beschwerdeführers und anschließender Fahrerflucht seitens des Beschwerdegegners kam. Der Vorfall wurde vom Beschwerdeführer dabei mittels einer in seinem Fahrzeug installierten Dashcam-Anlage aufgezeichnet. Diese Anlage filmte den vorderen und hinteren Fahrbahnbereich der Straße, sodass im konkreten Fall das Kennzeichen des kollidierenden Fahrzeugs erkennbar war, Personen jedoch nicht. Die angefertigten Bilder würden sich grundsätzliche alle drei Minuten selbst überschreiben, außer der Beschwerdeführer zieht im Falle eines Unfalles eine Karte heraus, was hier nach der Kollision geschehen ist.

Daraufhin wurde dem Beschwerdeführer in einem Straferkenntnis der Datenschutzbehörde aufgrund der Verletzung von Art 5 Abs 1 lit a und c sowie Art 6 Abs 1 DSGVO eine Geldbuße erteilt. Die Videoüberwachung sei nicht auf Bereiche beschränkt gewesen, welche in der ausschließlichen Verfügungsbefugnis des Verantwortlichen standen, weshalb die Bildverarbeitung somit nicht dem Zweck angemessen und nicht auf das notwendige Maß begrenzt gewesen sei.

Rechtliche Beurteilung:

Das BVwG führte aus, dass Art 6 Abs 1 lit f DSGVO zwei kumulative Voraussetzungen vorsieht, damit eine Verarbeitung personenbezogener Daten rechtmäßig ist, und zwar zum einen, dass die Verarbeitung personenbezogener Daten zur Verwirklichung des berechtigten Interesses überhaupt erforderlich ist, und zum anderen, dass nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person(en) überwiegen.

Der Verwaltungsgerichtshof (VwGH) führte in einer ähnlichen Entscheidung in der Vergangenheit bereits aus, dass allein aus dem Umstand, dass öffentlicher Raum gefilmt werde, für sich genommen nicht auf das Fehlen einer entsprechenden rechtlichen Befugnis geschlossen werden könne und stützte sich dabei u.a. maßgeblich auf den Schlussantrag von Generalanwalt Jääskinen in der Sache Ryneš [6]. Dem folgte der OGH und stellte fest, dass es jedenfalls einer Interessensabwägung bedarf, wobei in § 12 Abs 3 Z 1 und Z 2 DSG der vorbeugende Schutz des Eigentums und des Lebens unter näher dargestellten Voraussetzungen sogar ausdrücklich als (überwiegend) berechtigtes Interesse bei Bildverarbeitung im öffentlichen Raum qualifiziert wurde.

Dass an der (Bild)Dokumentation eines konkreten Unfallgeschehens schon allein zum Zweck der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen ein erhebliches Interesse eines Unfallbeteiligten besteht, kann nach Ansicht des OGH nicht in Zweifel gezogen werden. Demgegenüber sei ein generelles überwiegendes Interesse von Personen im Straßenverkehr, nicht gefilmt zu werden, im Falle eines konkreten Unfallgeschehens und damit in einer Konstellation wie der vorliegenden

könne nicht angenommen werden. Der OGH betonte, dass es sich bei der Bewertung der rechtlichen Zulässigkeit von Bildverarbeitung mittels Dashcam stets eine Einzelfallbeurteilung notwendig sei.

Datenschutzbehörde:
Die Datenschutzbehörde erhob gegen das gegenständliche Erkenntnis Amts-revision. Sie ist jedoch vorläufig von ihrer Ansicht, dass die Videoüberwachung öffentlichen Raums zu privaten Zwecken mittels Dashcams jedenfalls unzulässig sei, abgewichen. [7] In einem aktualisierten FAQ legt die DSB einige Kriterien fest, welche eine Zulässigkeit von Dashcams indizieren können. Gleichzeitig weist die DSB dennoch darauf hin, dass die meisten Einsätze solcher Systeme im Regelfall unzulässig sein werden. [8]

Fazit:
Für den Einsatz von Dashcams auf österreichischen Straßen stellt diese Entscheidung vorerst jedenfalls eine Erleichterung dar. Gleichzeitig ist jedoch zu beachten, dass die meisten kommerziell erhältlichen Dashcams den strengen Anforderungen und dem restriktiven Zugang der DSB nicht gerecht werden.

Bildverarbeitung ohne Zugriff auf die Daten

In einem Erkenntnis vom 3.9.2019 behandelte das BVwG die Zurechenbarkeit einer Bildverarbeitung, auf die der Verarbeitende zu keinem Zeitpunkt Zugriff hatte. [9]

Sachverhalt:
Fußballspielerinnen eines Damenfußballvereins bemerkten, dass ihr Trainer heimlich nach dem Training ein Video von ihnen während dem Duschen anfertigte. Sie entdeckten das versteckte Handy, löschten das Video und wandten sich an die DSB, welche der Beschwerde stattgab.

Der Fußballtrainer erhob dagegen Beschwerde an das BVwG. Für eine mögliche Verletzung des Rechts auf Geheimhaltung hätte zumindest die Möglichkeit bestehen müssen, in irgendeiner Form Zugriff auf die Daten zu haben, was gegenständlich jedoch nicht gegeben war, da die Betroffenen das Handy nach der Entdeckung beschlagnahmt und das Video darauf sofort gelöscht hatten.

Rechtliche Beurteilung:

Nach Ansicht des BVwG sei es nicht relevant, ob der Beschwerdeführer nach der Anfertigung auch Kenntnis von der Aufnahme erhalten hatte. Entscheidend für die Zuweisung der Verantwortlichkeit sei vielmehr, wer über die wesentlichen Aspekte der Mittel der Verarbeitung entscheidet. Für die Zuschreibung war es nicht erforderlich, dass der Verantwortliche selbst Daten verarbeitete, sich im Besitz der Daten befand oder über die physische Herrschaft verfügte. Außerdem fällt unter den Begriff der Verarbeitung bereits das Erheben von Daten und werden gemäß § 13 Abs 2 DSG sogar Fälle der bloßen Echtzeitüberwachung (ohne Speicherung) als Bildaufnahme qualifiziert. Die Bildverarbeitung wurde daher dem Fußballtrainer zugerechnet und eine Verletzung des Rechts auf Geheimhaltung festgestellt.

Fazit:
Solange die wesentlichen Entscheidungen über Mittel und Zweck bei demjenigen liegen, der das System zur Bildverarbeitung installiert hat, kann auch ein fehlender Zugriff auf die Bilddaten eine datenschutzrechtliche Verantwortlichkeit nicht beseitigen. Während das Kontrollverhältnis im

vorliegenden Fall offensichtlich war, können diese Erkenntnisse auch auf komplexere Sachverhalte umgelegt werden, insbesondere auch auf jene, in denen überhaupt keine Speicherung – sondern nur ein Erheben – der Daten stattfinden.

[1] BVwG 25.11.2019, W211 2210458-1.
[2] BVwG 20.11.2019, W256 2214855-1.
[3] DSB Newsletter 1/2020, abrufbar unter https://www.dsb.gv.at/newsletter.
[4] OGH 27.11.2019, 6 Ob 150/19f.
[5] BVwG 16.10.2019, W256 2222862-1.
[6] GA 10.6.2014, C-212/13 (Ryneš), Rz 63 ff.
[7] DSB Newsletter 1/2020, abrufbar unter https://www.dsb.gv.at/newsletter.
[8] https://www.dsb.gv.at/fragen-und-antworten#Dashcams_Autokameras.
[9] BVwG 3.9.2019, W214 2219944-1.

Österreichische Datenschutzbehörde legt Verordnungsentwurf für datenschutzrechtliche Zertifizierungen vor

Beitrag verfasst von Mag. Maximilian Kröpfl am 07.05.2020 – KTR-Newsletter Juni 2020

Die Datenschutz-Grundverordnung unterscheidet zwischen bloß privaten Zertifikaten und echten DSGVO-Datenschutzzertifikaten, -prüfzeichen und -siegeln. Die österreichische Datenschutzbehörde hat diese Woche ihren Entwurf für eine Verordnung über die Anforderungen an die Akkreditierung einer Zertifizierungsstelle (Zertifizierungsstellen-Akkreditierungs-Verordnung; kurz: ZeStAkk-V) mit der Bitte um Stellungnahmen an einen ausgewählten Expertenkreis ausgesandt.

Was wird zertifiziert?

Gegenstand einer genehmigten datenschutzrechtlichen Zertifizierung ist immer eine Datenverarbeitung im Zusammenhang mit personenbezogenen Daten. Vor dem Hintergrund, dass eine Prüfung der Datenverarbeitung auch die eingesetzten technischen Systeme sowie die Verarbeitungsorganisation umfasst, werden Hard- und Software sowie getroffene technischen und organisatorische Maßnahmen (wie ein Datenschutzmanagementsystem) mittelbar geprüft und zertifiziert. Wenngleich auch nur Teilbereiche einer Datenverarbeitung zertifizierungsfähig sind, sind Organisationen oder Verantwortliche bzw. Auftragsverarbeiter in ihrer Gesamtheit nicht zertifizierungsfähig.

Eine solche datenschutzrechtliche Zertifizierung ist für drei Jahre gültig. Während dieses Zertifizierungszeitraums hat die Zertifizierungsstelle ein Überwachungsaudit durchzuführen. Dieses soll sicherstellen, dass Verantwortliche oder Auftragsverarbeiter die Zertifizierungskriterien dauerhaft und nicht bloß zum (Re-)Zertifizierungszeitpunkt vollumfänglich einhalten. Wenngleich der Verordnungsentwurf über die Frequenz dieser Überwachungsaudits schweigt, lässt ein Blick nach Deutschland vermuten, dass zumindest ein Überwachungsaudit pro Zertifizierungszeitraum erwartet wird.

Wozu Zertifizierung?

Mit solchen genehmigten datenschutzrechtlichen Zertifizierungen sollen die Transparenz im Zusammenhang mit der Verarbeitung personenbezogener Daten erhöht und die Einhaltung der DSGVO verbessert werden. So können datenschutzspezifische Zertifizierungsverfahren sowie Datenschutzsiegel und -prüfzeichen als Faktoren herangezogen werden, um die Erfüllung der Pflichten des Verantwortlichen oder die korrekte Implementierung von technischen und organisatorischen Maßnahmen nachzuweisen. Darüber hinaus können datenschutzrechtliche Zertifizierungen geeignete Garantien für den internationalen Datentransfer darstellen. Sollte bei der Einhaltung des Datenschutzes doch einmal etwas schiefgehen, so hat die Datenschutzbehörde das Bestehen einer datenschutzrechtlichen Zertifizierung bei der Entscheidung über das Verhängen einer Geldstrafe oder der Festsetzung der Strafhöhe gebührend zu berücksichtigen. Alle diese Vorteile gelten freilich nur für aufrechte genehmigte datenschutzrechtliche Zertifizierungen.

Doch wie helfen datenschutzrechtliche Zertifizierungen in der täglichen Unternehmenspraxis? Eine datenschutzrechtliche Zertifizierung kann beim Nachweis guter datenschutzrechtlicher Praxis unterstützen. Darüber hinaus kann sie die Auswahl von Auftragsverarbeitern nicht nur effizienter, sondern auch kostengünstiger gestalten. Das Vorliegen einer datenschutzrechtlichen Zertifizierung gibt dem Unternehmen als Verantwortlichem die Sicherheit, dass der zertifizierte Umfang den genehmigten Zertifizierungskriterien entspricht. Deshalb bringt eine Zertifizierung überdies einen Wettbewerbsvorteil für all jene Brachen, die regelmäßig als Auftragsverarbeiter tätig werden. Wer ein Zertifikat, Prüfzeichen oder Siegel zum Nachweis genehmigter datenschutzrechtlicher Konformität vorweisen kann, ist der Konkurrenz einen Schritt voraus.

Doch kommen die Kosten der Zertifizierung auch wieder herein? Sieht man über datenschutzrechtliche Zertifizierungen hinaus, so zeigen Studien, dass Produkte und Dienstleistungen, die mit einem Zertifikat werben, regelmäßig höhere Preise erzielen. So haben Erhebungen ergeben, dass die Zertifizierung von Bio-Milch zu einem Preisanstieg von 40 % führte, bei Rindfleisch entsprechend um 22 %. Die Zertifizierung einer E-Commerce-Webseite rechtfertigte eine höhere Marge von durchschnittlich 1,5 %.

Wir bei Knyrim Trieb Rechtsanwälte sehen ein großes Potential in der datenschutzrechtlichen Zertifizierung. Durch die jahrelange Zusammenarbeit mit Unternehmen aller Branchen und aller Größen wissen wir, wie aufwändig gutes Datenschutzmanagement ist. Gerade im Dienstleistungsbereich erhoffen wir uns von guten und vertrauenswürdigen genehmigten Zertifikaten eine Erleichterung für die vielen Experten ihres Faches, die regelmäßig als datenschutzrechtliche Auftragsverarbeiter tätig werden. Wir informieren Sie gerne und stehen Ihnen mit Rat, Tat und Passion zur Seite.

HINWEIS

Daniela Flickentanz bei F*** Up Show von Matthias Strolz auf PULS4

Wer hätte gedacht, dass Frau Flickentanz, welche ihre erste Live-Uraufführung ihres Songs „Daten, oh yeah!“ vor Publikum 2018 bei unserer Buchpräsentation „Der DatKomm“ in der Albert

Halle in Wien hatte, ihren DSGVO-Song nun bereits bei Matthias Strolz im Fernsehen präsentieren darf!

Den Link zur Show findet sich **HIER**
(Daniela Flickentanz zu sehen ab Minute 17:15, wo sie auch über die Manz-Präsentation berichtet!)

---

8. Juni 2020 - WEBINAR

Microsoft 365 Virtual Training Day:
Meeting Organizational Compliance Requirements

Im Rahmen des kostenlosen Webinars erfahren Sie, wie Sie sowohl Ihre IT schützen als auch rechtskonform und kostensparend arbeiten können. Wir laden Sie auch sehr herzlich ein Ihre individuellen Fragen an unsere ExpertInnen zu stellen.

Der Microsoft 365 Virtual Training Day richtet sich vorrangig an IT-ExpertInnen, Rechts- und Compliance-Manager, sowie an CISOs und Sicherheitsbeauftragte.

Das Programm finden Sie HIER

Termin: 8. Juni 2020 – 09.00-11.15 Uhr
Ort: Online
Anmeldung: online unter resources.office.com

Weitere Newsletter finden Sie auf unserer Webseite: www.kt.at/newsletter
Erfahren Sie mehr über aktuellen Veranstaltungen auf unserer Webseite: www.kt.at/termine

---

Knyrim Trieb Rechtsanwälte OG

Mariahilfer Straße 89a, A-1060 Wien, T: +43 1 909 30 70, F: +43 1 909 36 39
FB: knyrimtrieb E: ky@kt.at, W: www.kt.at

FN 462250f, HG Wien