DATENSCHUTZSTELLE
FÜRSTENTUM LIECHTENSTEIN

Judikaturspiegel zum europäischen Datenschutzrecht

Ausgewählte Entscheidungen Europäischer Gerichte und Höchstgerichte

(2018 – 2024)

Vorbemerkung

Der europäische Gesetzgeber verfolgte mit der DSGVO und der DSRL-PJ die weitestgehende Harmonisierung des europäischen Datenschutzrechts. Trotz ihres Inkrafttretens sind weiterhin Unterschiede in der nationalen Vollzugspraxis und Rechtsprechung festzustellen.

Im Wege der Rechtsvergleichung können wertvolle Erkenntnisse für die eigene Vollzugspraxis und die Anwendung des Datenschutzrechts gewonnen werden; auch um die Eigenheiten des nationalen Rechtsstandes zu ermitteln und abgrenzen zu können.

Der vorliegende «Judikaturspiegel» dient dazu, ausgewählte Gerichtsentscheide aus Mitgliedstaaten des EWR sowie der EU (aus dem Zeitraum 2018 bis Dezember 2024) in Kurzfassung vorzustellen bzw. wesentliche Passagen der Entscheidungen hervorzuheben. Es besteht dabei kein Anspruch auf Vollständigkeit. Die angeführten Entscheidungen nationaler Gerichte und Höchstgerichte sowie des Europäischen Gerichtshofs (EuGH) bergen für die Anwendung und Vollzugspraxis der DSGVO und des europäischen Datenschutzrechts im weiteren Sinne durchwegs interessante Erkenntnisse. Diese zeichnen die internationale Entwicklung des europäischen Datenschutzrechts vor und können im Wege der Rechtsvergleichung auch für die liechtensteinische Rechtslage bedeutende Aufschlüsse bereithalten, auch wenn sich deren Ausführungen nicht allesamt vorbehaltlos für inländische Rechtssachen übernehmen lassen.

Unberücksichtigt blieb die Rechtsprechung des EGMR. Eine Zusammenfassung der EGMR-Rechtsprechung zu Art. 8 EMRK (Recht auf Wahrung des Privat- und Familienlebens) finden Sie über: https://www.coe.int/en/web/data-protection/echr-case-law (Stand Dezember 2024).

Zur leichteren Handhabung wurden die jeweiligen Fundstellen der Entscheidungen via Hyperlink in den Untertiteln eingearbeitet. Dies, sowie die ein einigen Fällen zusätzlich angeführten und verlinkten Quellen, ermöglichen es den interessierten Leserinnen und Lesern, leichter weitergehende Informationen zur betreffenden Entscheidung zu erlangen.

Die Datenschutzstelle verfolgt mit der vorliegenden Übersicht ihren Aufklärungsauftrag. Anzumerken bleibt, dass sich dieser Judikaturspiegel auf eine deskriptive Darstellung wesentlicher Teile und Auszüge ausgewählter Entscheidungen beschränkt und keine analytische Judikatur-Besprechung oder Glossierung zur Hand geben soll. Ausserdem kann keine Haftung für fehlerhafte Übersetzungen fremdsprachiger Judikatur und rechtsirrige Darstellung ausländischer Bestimmungen übernommen werden.

In der vorliegenden, aktualisierten Version des Judikaturspiegels finden Sie wie bisher ausgewählte Entscheidungen von Gerichten und Höchstgerichten aus Liechtenstein, Deutschland, Österreich und Frankreich sowie ein neues Kapitel über Entscheidungen des EuGH. Mit Ausnahme des Kapitels zu Frankreich wurden die Kapitel zu Liechtenstein, Deutschland und Österreich mit aktueller Rechtsprechung ergänzt (Stichtag 31. Dezember 2024). Die eingefügten Passagen sind zur leichteren Orientierung **blau** eingefärbt. Durch neue Rechtsprechung widerlegte und damit überholte Judikatur wurde aus der vorliegenden Fassung entfernt. Zudem wurden kleine formale Anpassungen vorgenommen.

Inhaltsübersicht

I. LIECHTENSTEIN

A. Verwaltungsgerichtshof (VGH)

a. Urteile des VGH vom 3. September 2021, Nr. 2021/031 und 2021/032 – Anonymität Beschwerdeführer

Unter bestimmten Umständen muss die Identität eines Beschwerdeführers gegenüber dem Verantwortlichen nicht offengelegt werden.

Die Identität des Beschwerdeführers bei einer Beschwerde nach Art. 77 DSGVO muss dem Verantwortlichen nicht grundsätzlich offengelegt werden. Es muss im Einzelfall erörtert werden, ob die Zurückhaltung der Identität die Ausübung der Verteidigungsrechte des Verantwortlichen behindert oder die Erfüllung der Vorgaben der DSGVO. Diese Einschätzung wird von der Datenschutzbehörde vorgenommen, sie entscheidet über die Zurückbehaltung der Identität. Im vorliegenden Fall kritisierte die Datenschutzstelle eine standardisierte Datenverarbeitung der Verantwortlichen und sprach Empfehlungen aus, die ohne Offenlegung der Identität umgesetzt werden konnten. Die Identität des Beschwerdeführers wurde dem Verantwortlichen nicht offengelegt.

Vorlagefrage an den EFTA-Gerichtshof:

Am 10. Dezember 2020 entschied der EFTA-Gerichtshof bezüglich zweier Vorabentscheidungsersuchen der Liechtensteinischen Beschwerdekommission für Verwaltungsangelegenheiten («joined cases» E-11/19 und E-12/19) zur Klärung der Frage, ob sich die Unentgeltlichkeit des Beschwerdeverfahrens nach Artikel 77 der DSGVO auch auf anschliessende Verfahren vor Rechtsmittelinstanzen erstreckt, sowie zur Frage, ob bei einer Beschwerde die betroffene Person gegenüber dem Beschwerdegegner genannt werden muss.

Zusammengefasst sprach der EFTA-Gerichtshof aus, dass eine allfällige Zurückhaltung personenbezogener Daten eines Beschwerdeführers im Verwaltungsverfahren anhand von Art. 5 und 6 DSGVO zu prüfen ist. Ein Zurückhalten dürfe nicht erfolgen, wenn es die Erfüllung von Pflichten nach der DSGVO, das Recht auf wirksamen Rechtsbehelf oder ein ordnungsgemässes Verfahren behindern würde (Spruchpunkt 1). Darüber hinaus dürfen einer betroffenen Person, die anlässlich des Rechtsbehelfs eines Verantwortlichen zur Partei eines Verfahrens gemäss Art. 78 Abs. 1 DSGVO wird, keinerlei Kosten im Zusammenhang mit diesem Verfahren auferlegt werden (Spruchpunkt 2).

Quelle: Entscheidung des EFTA-Gerichtshofs vom 10. Dezember 2020, Joined Cases E-11/19 and E-12/19

b. Urteil des VGH vom 15. Dezember 2023, Nr. 2022/109 – Videoüberwachung Freizeitanlagen

Die Videoüberwachung von Freizeitanlagen ist nur in sehr begrenztem Ausmass möglich.

Eine Liechtensteiner Gemeinde installierte zur Bekämpfung vermehrter Vandalismusvorfälle auf einer von ihr betriebenen Freizeitanlage ein umfassendes Überwachungskamerasystem. Der Betrieb dieser Videokameras wurde von der Datenschutzstelle mit Verfügung eingeschränkt bzw. in gewissen Teilen untersagt, weil er überschiessend und nicht datenschutzkonform durchgeführt wurde. Im Beschwerdeverfahren wurde die Entscheidung schliesslich dem VGH vorgelegt, der die Verfügung der Datenschutzstelle bestätigte und der Gemeinde die Umsetzung der Einschränkungen auferlegte.

Bei der Prüfung, ob die Videoüberwachung die Zulässigkeitskriterien gemäss Art. 5 Abs. 1 DSG erfüllt, also geeignet, erforderlich und zumutbar ist, um ein bestimmtes im öffentlichen Interesse liegendes Ziel zu erreichen, stimmt der VHG der Beurteilung der Datenschutzstelle zu. Die Zumutbarkeit ist nicht gegeben. Das Interesse der betroffenen Personen, die Freizeitanlage unüberwacht zu nutzen, überwiegt das berechtigte Interesse der Gemeinde zur Videoüberwachung weitestgehend. Davon ausgenommen und damit erlaubt wird ausschliesslich der Überwachungsbetrieb bei Nacht sowie bei einem spezifischen, abgegrenzten Problembereich.

Beim zulässigen (nächtlichen) Betrieb der Videokameras ist auf eine angemessen kurze Speicherdauer zu achten entsprechend Art. 5 Abs. 1 Bst. e DSGVO.

B. Staatsgerichtshof (StGH)

a. Urteil des StGH vom 26. März 2024, Nr. 2023/106 – PEID-Nummer

Die PEID-Nummern werden automatisch generiert und enthalten keine personenbezogenen Daten.

Die Beschwerdeführerin fand in der Zahlenfolge ihrer PEID-Nummer eine Variation ihres Geburtsdatums sowie anderer personenbezogene Daten und verlangte eine Änderung, um Verwechslungen zu vermeiden und ihr Recht auf Datenschutz geltend zu machen. Der StGH urteilte, dass keine datenschutzrechtliche Problematik ersichtlich sei. Die PEID-Nummer beinhalte keine personenbezogenen Daten, da sie automatisch generiert werde. Zufällige Übereinstimmungen mit persönlichen Daten würden folglich keine Verletzung der Privatsphäre darstellen.

b. Urteil des StGH vom 26. Juni 2023, Nr. 2023/016 – Gerichtsstand für Löschungsbegehren

Eine Toplevel-Domain in einem anderen Staat als demjenigen des Sitzes der Gesellschaft führt nicht automatisch zu einer Änderung des Gerichtsstandes.

Eine Beschwerdeführerin war der Ansicht, dass eine Top-Level-Domain .li in Verbindung mit Art. 17 und Art. 82 Abs. 6 DSGVO die Zuständigkeit des Landgerichts zur Behandlung ihres Löschungsbegehrens begründe, obwohl die Beklagte ihren Sitz in Irland hat. Die Gerichte teilten diese Ansicht nicht.

c. Urteil des StGH vom 2. September 2024, Nr. 2024/056 – Arbeitsrecht und Datenschutzbeauftragte

Abberufung vs. Kündigung eines Datenschutzbeauftragten

Art. 38 Abs. 3 DSGVO und Art. 7 Abs. 3 DSG schützen die Datenschutzbeauftragten vor einer Abberufung aufgrund der Erfüllung ihrer Aufgaben. Dieser Schutz führt jedoch nicht zu einer «Pragmatisierung». Von der Abberufung zu unterscheiden ist nämlich die Kündigung. Eine ordentliche Kündigung unter Einhaltung der Kündigungsfrist ist jedenfalls immer dann zulässig, wenn die Kündigung unbestrittenermassen unabhängig von der Ausübung der Datenschutzfunktion und somit auch nicht als sogenannte Rachekündigung erfolgt.

II. DEUTSCHLAND

A. Bundesverfassungsgericht (BVerfGE)

a. Beschluss der 2. Kammer des Ersten Senats vom 19. März 2020, 1 BvQ 1/20 – Krankenversicherungsdaten

Nutzung von Krankenversicherungsdaten nach Pseudonymisierung/Anonymisierung ist zulässig.

«Mit (ihrem am 19. Mai 2020 veröffentlichten) Beschluss hat die 2. Kammer des Ersten Senats einen Antrag auf vorläufige Ausserkraftsetzung des Vollzugs neu in das SGB V ein-gefügter Vorschriften **abgelehnt, die die Nutzung von Daten gesetzlich Krankenversicherter in pseudonymisierter oder anonymisierter Form im Hinblick auf digitale Innovationen und für weitere Zwecke, unter anderem zur medizinischen Forschung, ermöglichen**. Das Ver-fahren wirft schwierige verfassungsrechtliche Fragen auf, über die im Eilverfahren inhaltlich nicht entschieden werden kann. Die Kammer hatte deshalb aufgrund summarischer Prüfung im Rahmen einer Folgenabwägung zu entscheiden und den für die Prüfung der vorläufigen Ausserkraftsetzung eines Gesetzes geltenden strengen Massstab anzuwenden. Die Nachteile, die sich aus einer vorläufigen Anwendung der Vorschriften ergeben, wenn sich das Gesetz im Nachhinein als verfassungswidrig erwiese, sind nach Ansicht der Kammer zwar von erheblichem Gewicht. Sie überwiegen aber nicht deutlich die Nachteile, die entstünden, wenn die Vorschriften ausser Kraft träten, sich das Gesetz aber später als verfassungsgemäss erwiese.»

(Hervorhebungen nicht im Original)

Quelle: Pressemitteilung Nr. 29/2020 vom 30. April 2020

b. Urteil des Ersten Senats vom 19. Mai 2020, 1 BvR 2835/17 – Bestandsdaten, Fernmeldeaufklärung

Ausland-Ausland-Fernmeldeaufklärung nach dem BND-Gesetz verstiess gegen Grundrechte des deutschen Grundgesetzes.

«(D)ie **Überwachung der Telekommunikation von Ausländern** im Ausland durch den Bundesnachrichtendienst (ist) an die Grundrechte des Grundgesetzes gebunden (…) und **(verstösst) nach der derzeitigen Ausgestaltung der Ermächtigungsgrundlagen gegen das grundrechtliche Telekommunikationsgeheimnis** (Art. 10 Abs. 1 GG) und die Pressefreiheit (Art. 5 Abs. 1 Satz 2 GG) (…). Dies betrifft sowohl die Erhebung und Verarbeitung der Daten als auch die Übermittlung der hierdurch gewonnenen Daten an andere Stellen wie ebenfalls die Kooperation mit anderen ausländischen Nachrichtendiensten. Eine verfassungsmässige Ausgestaltung der gesetzlichen Grundlagen der Ausland-Ausland-Fernmeldeaufklärung (auch: „Ausland-Ausland-Telekommunikationsüberwachung“) ist jedoch möglich.

Nach der Entscheidung ist die **Bindung der deutschen Staatsgewalt an die Grundrechte** nach Art. 1 Abs. 3 GG **nicht auf das deutsche Staatsgebiet** begrenzt. Jedenfalls der Schutz des Art. 10 Abs. 1 und des Art. 5 Abs. 1 Satz 2 GG als **Abwehrrechte gegenüber einer**

Telekommunikationsüberwachung erstreckt sich auch auf Ausländer im Ausland. Das gilt unabhängig davon, ob die Überwachung vom Inland oder vom Ausland aus erfolgt. Da der Gesetzgeber demgegenüber von der Unanwendbarkeit der Grundrechte ausgegangen ist, hat er den hieraus folgenden Anforderungen weder in formeller noch in inhaltlicher Hinsicht Rechnung getragen. (…) Insbesondere ist die Überwachung nicht auf hinreichend bestimmte Zwecke begrenzt und durch diese kontrollfähig strukturiert; auch fehlt es an verschiedenen Schutzvorkehrungen, etwa zum Schutz von Journalisten oder Rechtsanwälten. Hinsichtlich der Datenübermittlung fehlt es neben anderem an der Gewährleistung eines hinreichend gewichtigen Rechtsgüterschutzes und ausreichender Eingriffsschwellen. Entsprechend **enthalten** die Vorschriften zu den Kooperationen mit ausländischen Nachrichtendiensten **keine hinreichenden Begrenzungen und Schutzvorkehrungen**. Hinsichtlich all dieser Befugnisse fehlt es zudem an einer ausgebauten unabhängigen objektivrechtlichen Kontrolle. Eine solche Kontrolle muss als kontinuierliche Rechtskontrolle ausgestaltet sein und einen umfassenden Kontrollzugriff ermöglichen.

Bei verhältnismässiger Ausgestaltung ist das Instrument der strategischen Ausland-Ausland-Telekommunikationsüberwachung demgegenüber mit den Grundrechten des Grundgesetzes im Grundsatz vereinbar. Die beanstandeten Vorschriften gelten daher bis zum Jahresende 2021 fort, um dem Gesetzgeber eine Neuregelung unter Berücksichtigung der grundrechtlichen Anforderungen zu ermöglichen.»

(Hervorhebungen nicht im Original)

Quelle: Pressemitteilung Nr. 37/2020 vom 19. Mai 2020

c. Beschluss des Ersten Senats vom 27. Mai 2020, 1 BvR 1873/13 und 1 BvR 2618/13 – Bestandsdatenauskunft

Regelungen zur Bestandsdatenauskunft in Deutschland waren verfassungswidrig.

§ 113 des Telekommunikationsgesetzes (TKG) und mehrere Fachgesetze des Bundes «verletzen die beschwerdeführenden Inhaber von Telefon- und Internetanschlüssen in ihren Grundrechten auf informationelle Selbstbestimmung sowie auf Wahrung des Telekommunikationsgeheimnisses (Art. 10 Abs. 1 GG). **Die manuelle Bestandsdatenauskunft ermöglicht es Sicherheitsbehörden, von Telekommunikationsunternehmen Auskunft insbesondere über den Anschlussinhaber eines Telefonanschlusses oder einer zu einem bestimmten Zeitpunkt zugewiesenen IP-Adresse zu erlangen**. Mitgeteilt werden personenbezogene Daten der Kunden, die im Zusammenhang mit dem Abschluss oder der Durchführung von Verträgen stehen (sogenannte Bestandsdaten). Nicht mitgeteilt werden dagegen Daten, die sich auf die Nutzung von Telekommunikationsdiensten (sogenannte Verkehrsdaten) oder den Inhalt von Kommunikationsvorgängen beziehen.

Die Erteilung einer Auskunft über Bestandsdaten ist grundsätzlich nach deutschem Verfassungsrecht zulässig. Der Gesetzgeber muss aber nach dem Bild einer Doppeltür sowohl für die Übermittlung der Bestandsdaten durch die Telekommunikationsanbieter als auch für den Abruf dieser Daten durch die Behörden jeweils verhältnismässige Rechtsgrundlagen schaffen. Übermittlungs- und Abrufregelungen müssen die Verwendungszwecke der Daten

hinreichend begrenzen, indem sie insbesondere tatbestandliche Eingriffsschwellen und einen hinreichend gewichtigen Rechtsgüterschutz vorsehen. Der Senat hat klargestellt, dass die allgemeinen Befugnisse zur Übermittlung und zum Abruf von Bestandsdaten trotz ihres gemässigten Eingriffsgewichts für die Gefahrenabwehr und die Tätigkeit der Nachrichtendienste grundsätzlich einer im Einzelfall vorliegenden konkreten Gefahr und für die Strafverfolgung eines Anfangsverdachts bedürfen. **Findet eine Zuordnung dynamischer IP-Adressen statt, muss diese im Hinblick auf ihr erhöhtes Eingriffsgewicht darüber hinaus auch dem Schutz oder der Bewehrung von Rechtsgütern von zumindest hervorgehobenem Gewicht dienen.** Bleiben die Eingriffsschwellen im Bereich der Gefahrenabwehr oder der nachrichtendienstlichen Tätigkeit hinter dem Erfordernis einer konkreten Gefahr zurück, müssen im Gegenzug erhöhte Anforderungen an das Gewicht der zu schützenden Rechtsgüter vorgesehen werden. **Die genannten Voraussetzungen wurden von den angegriffenen Vorschriften weitgehend nicht erfüllt.** Im Übrigen hat der Senat wiederholend festgestellt, dass eine Auskunft über Zugangsdaten nur dann erteilt werden darf, wenn die gesetzlichen Voraussetzungen für ihre Nutzung gegeben sind.»

(Hervorhebungen nicht im Original)

Quelle: Pressemitteilung Nr. 61/2020 vom 17. Juli 2020

B. Bundesverwaltungsgericht (BVerwG)

a. Urteil des BVerwG vom 16. September 2020, Nr. Az.: 6 C 10.19 – Auskunftsanspruch

Der Datenschutzrechtliche Auskunftsanspruch ist ein höchstpersönliches Recht. Das Recht aus Art. 15 DSGVO kann daher nicht durch Dritte ausgeübt werden.

« […] Sinn und Zweck des Auskunftsanspruchs aus Art. 15 Abs. 1 DSGVO sprechen gegen ein Verständnis des Begriffs der betroffenen Person, das den Kläger in seiner Funktion als Insolvenzverwalter umfassen würde. Anlass und Regelungsziel der DSGVO ist der in Art. 8 Abs. 1 GRCh und Art. 16 Abs. 1 AEUV gewährleistete Schutz natürlicher Personen bei der Verarbeitung der sie betreffenden personenbezogenen Daten (Art. 1 Abs. 2 DSGVO und Erwägungsgrund 1). Bereits auf der Ebene der Grundrechtecharta ist das Recht jeder Person verankert, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken (Art. 8 Abs. 2 Satz 2 GRCh). Die Betroffenenrechte der Datenschutz-Grundverordnung wurzeln in der Erwägung des europäischen Normgebers, dass der Einzelne selbst über die Preisgabe und Verwendung seiner persönlichen Daten bestimmen können muss. Natürliche Personen sollen daher grundsätzlich die Kontrolle über ihre eigenen Daten besitzen (Erwägungsgrund 7 Satz 2). Zu diesem Zweck räumen Art. 8 Abs. 2 GRCh und Art. 15 Abs. 1 DSGVO der betroffenen Person ein Auskunftsrecht darüber ein, welche personenbezogenen Daten von Dritten erhoben worden sind. Ziel ist es, dass sich der Betroffene der Verarbeitung bewusst ist und auf dieser Grundlage deren Rechtmässigkeit überprüfen kann (Erwägungsgrund 63 Satz 1). Das Auskunftsrecht aus Art. 15 Abs. 1 DSGVO und das Recht auf Erhalt einer Kopie gemäss Absatz 3 der Vorschrift erweisen sich damit als elementare subjektive Datenschutzrechte, da erst die Kenntnis darüber, ob und in welchem Umfang ein

Verantwortlicher personenbezogene Daten verarbeitet, die betroffene Person in die Lage versetzt, weitere Rechte auszuüben.» (Urteil, Rz. 19)

Quelle: Pressemitteilung Nr. 51/2020 vom 17. September 2020

C. Bundesgerichtshof (BGH)

a. Urteil des I. Zivilsenats vom 28. Mai 2020, I ZR 7/16 – Cookie-Einwilligung

Einwilligungserfordernis für Cookies zur Erstellung von Nutzerprofilen

«Die Einholung der Einwilligung mittels eines voreingestellten Ankreuzkästchens war nach der bis zum 24. Mai 2018 geltenden Rechtslage - also vor Geltung der Verordnung (EU) 2016/679 - im Sinne von § 307 Abs. 2 Nr. 1 BGB mit wesentlichen Grundgedanken des § 15 Abs. 3 Satz 1 TMG unvereinbar. Der beanstandete Einsatz von Cookies durch die Beklagte als Diensteanbieter dient, wie von § 15 Abs. 3 Satz 1 TMG vorausgesetzt, der Erstellung von Nutzerprofilen zum Zwecke der Werbung, indem das Verhalten des Nutzers im Internet erfasst und zur Zusendung darauf abgestimmter Werbung verwendet werden soll. Bei der im Streitfall in den Cookies gespeicherten zufallsgenerierten Nummer (ID), die den Registrierungsdaten des Nutzers zugeordnet ist, handelt es sich um ein Pseudonym im Sinne dieser Vorschrift. § 15 Abs. 3 Satz 1 TMG ist mit Blick auf Art. 5 Abs. 3 Satz 1 der Richtlinie 2002/58/EG in der durch Art. 2 Nr. 5 der Richtlinie 2009/136/EG geänderten Fassung dahin richtlinienkonform auszulegen, dass **für den Einsatz von Cookies zur Erstellung von Nutzerprofilen für Zwecke der Werbung oder Marktforschung die Einwilligung des Nutzers erforderlich** ist. Der Gerichtshof der Europäischen Union hat auf Vorlage durch den Senat entschieden, dass Art. 2 Buchst. f und Art. 5 Abs. 3 Satz 1 der Richtlinie 2002/58/EG in Verbindung mit Art. 2 Buchst. h der Richtlinie 95/46/EG dahin auszulegen sind, dass keine wirksame Einwilligung im Sinne dieser Bestimmungen vorliegt, wenn die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät des Nutzers einer Website gespeichert sind, mittels Cookies durch ein voreingestelltes Ankreuzkästchen erlaubt wird, das der Nutzer zur Verweigerung seiner Einwilligung abwählen muss. […]

An dieser Rechtslage hat sich seit dem 25. Mai 2018, dem ersten Geltungstag der Verordnung (EU) 2016/679, nichts geändert, weil diese Verordnung nach ihrem Art. 95 die Fortgeltung des § 15 Abs. 3 Satz 1 TMG als den Art. 5 Abs. 3 Satz 1 der Richtlinie 2002/58/EG umsetzende nationale Regelung unberührt lässt. **Soweit für die Definition der Einwilligung nicht mehr auf Art. 2 Buchst. h der aufgehobenen Richtlinie 95/46/EG abgestellt werden kann, sondern Art. 4 Nr. 11 der Verordnung (EU) 2016/679 heranzuziehen ist, führt dies zum selben Ergebnis.** Der Gerichtshof der Europäischen Union hat auf Vorlage durch den Senat auch mit Blick auf Art. 4 Nr. 11 der Verordnung (EU) 2016/679 entschieden, dass ein vom Nutzer abzuwählendes, voreingestelltes Ankreuzkästchen keine wirksame Einwilligung darstellt.»

(Hervorhebungen nicht im Original)

Quelle: Pressemitteilung Nr. 067/2020 vom 28. Mai 2020

Anmerkung: *Die für das deutsche Verfahren einschlägige RL 2009/136/EG wurde bisher (Stand: Dezember 2024) nicht ins EWR-Abkommen übernommen; es fehlt daher in*

Liechtenstein an einer nationalen Umsetzung (bspw. im KomG oder anderen einschlägigen Gesetzen). In Bezug auf die Einwilligung in Cookies zur Erstellung von Nutzerprofilen für Zwecke der Werbung oder Markforschung gilt in Liechtenstein jedoch dasselbe, wie im Urteil ausgeführt, da sich solche Cookies nicht mit dem berechtigten Interesse nach Art. 6 Abs. 1 Bst. f DSGVO rechtfertigen lassen.

b. Beschluss des Kartellsenats des Bundesgerichtshofs vom 23. Juni 2020, KVR 69/19 – Soziale Medien, Nutzerdaten

Kartellrechtliches Verbot einwilligungsloser Verarbeitung von Nutzerdaten durch Facebook

«Facebook verwendet Nutzungsbedingungen, die auch die Verarbeitung und Verwendung von Nutzerdaten vorsehen, die bei einer von der *Facebook*-Plattform unabhängigen Internetnutzung erfasst werden. **Das Bundeskartellamt hat Facebook untersagt, solche Daten ohne weitere Einwilligung der privaten Nutzer zu verarbeiten.** Der Kartellsenat des Bundes-gerichtshofs hat heute entschieden, dass dieses Verbot vom Bundeskartellamt durchgesetzt werden darf.»

(Hervorhebungen nicht im Original)

Quelle: Pressemitteilung Nr. 080/2020 vom 23. Juni 2020

c. Urteil des VI. Zivilsenats vom 22. Februar 2022, Nr. VI ZR 14/21 – Auskunftsrecht, Identität Hinweisgeber

Mietern kann das Auskunftsrecht über die Identität eines Nachbarn, der sich beschwert, zustehen. Auch wenn es sich um datenschutzrechtliche Informationen handele, seien die sich gegenüberstehenden Interessen der Parteien im Einzelfall abzuwägen.

«In die demnach vorzunehmende Abwägung zwischen den Interessen des Auskunftsberechtigten und des Hinweisgebers sind zugunsten des Auskunftsberechtigten Bedeutung, Gewicht und Zweck des Auskunftsrechts über die Herkunft der Daten gemäss Art. 15 Abs. 1 Halbsatz 2 Bst. g DS-GVO einzubeziehen. Das Recht jeder Person, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken, ist in Art. 8 Abs. 2 Satz 2 der Charta im Rahmen des Rechts auf Schutz personenbezogener Daten verbürgt**. Es dient dem Zweck, dass sich die betroffene Person der Verarbeitung der sie betreffenden Daten bewusst wird und deren Rechtmässigkeit überprüfen kann** (Erwägungsgrund 63 Satz 1). […] Das Auskunftsrecht gemäss Art. 15 Abs. 1 DS-GVO ist insbesondere erforderlich, um es der betroffenen Person gegebenenfalls zu ermöglichen, von dem für die Verarbeitung Verantwortlichen etwa die Berichtigung oder Löschung ihrer Daten zu verlangen (vgl. EuGH, Urteile vom 20. Dezember 2017 - Rs. C-434/16, NJW 2018, 757 Rn. 57 und vom 7. Mai 2009 - C-553/07, EuZW 2009, 546 Rn. 51 zur Richtlinie 95/46/EG). […]

Zugunsten des Hinweisgebers ist demgegenüber zu berücksichtigen, dass auch dessen Rechte durch Art. 7 Abs. 1 (Achtung des Privatlebens) und Art. 8 (Recht auf Schutz personenbezogener Daten) der Charta verbürgt sind, wobei diese beiden Grundrechte, soweit es um die

Verarbeitung personenbezogener Daten geht, eine einheitliche Schutzverbürgung bilden. […] Allerdings dürfen gemäss Art. 8 Abs. 2 Satz 1 der Charta seine Daten nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage (hier: Art. 6 Abs. 1 Satz 1 Bst. f DS-GVO) verarbeitet werden. **Allein der Einwand des auf Auskunft in Anspruch genommenen Verantwortlichen, dem Hinweisgeber - im Ergebnis ohne Rücksicht auf das Auskunftsrecht des Betroffenen - Vertraulichkeit zugesichert zu haben, führt noch nicht zum Recht, dem Auskunftsersuchenden die Information zu verweigern** […], ebenso wenig ein pauschaler Verweis auf das Schutzbedürfnis des Hinweisgebers und darauf, dass der Verantwortliche auf dessen Hinweise angewiesen sei. […]

Das Interesse an der Geheimhaltung des Hinweisgebers hat gegenüber dem Auskunftsinteresse regelmässig dann zurückzutreten, wenn der Hinweisgeber wider besseres Wissen oder leichtfertig unrichtige Angaben zu personenbezogenen Daten der betroffenen Person gemacht. […] Durch die Auskunft über die Identität des Hinweisgebers wird der Auskunftsberechtigte dann in die Lage versetzt, solche Ansprüche gegen die Person, von der die unrichtigen Daten herrühren, geltend zu machen.» (Urteil, Rz. 24-26)

(Hervorhebungen nicht im Original)

d. Urteil des VI. Zivilsenats vom 23. Mai 2023, Nr. VI ZR 476/18 – Voraussetzungen und Anforderungen eines Auslistungsanspruchs

Eine Auslistung erfordert keine - sei es vorläufige - Klärung der Richtigkeit des ausgelisteten Inhalts im Rahmen eines entsprechenden Rechtsbehelfs. Der Anspruchsteller muss für seinen Auslistungsantrag insoweit "nur" relevante und ausreichende Nachweise und Belege vorlegen.

Der Betreiber einer Suchmaschine ist verpflichtet, einem Auslistungsantrag stattzugeben, wenn die eine Auslistung begehrende Person relevante und hinreichende Nachweise vorlegt, die ihren Antrag zu stützen vermögen und belegen, dass die in dem aufgelisteten Inhalt enthaltenen Informationen offensichtlich unrichtig sind oder zumindest ein für diesen gesamten Inhalt nicht unbedeutender Teil dieser Informationen offensichtlich unrichtig ist.

Eine vorgängige Klärung der Richtigkeit des auszulistenden Inhalts ist somit nicht nötig.

Quelle: Pressemitteilung Nr. 084/2023 vom 23.05.2023

D. Bundessozialgericht

a. Urteil vom 8. Oktober 2019, B 1 A 3/19 R – Sozialdaten, Krankenkassen

Schutz von Sozialdaten verhindert Einbeziehung privater Dritter durch Krankenkassen.

«Eine Krankenkasse ist nicht berechtigt, ihren Versicherten in Konkurrenz zu Leistungen zugelassener Leistungserbringer eigene Leistungsangebote des Versorgungsmanagements zu

unterbreiten. Die Krankenkasse erfüllt den hierauf gerichteten Anspruch Versicherter mittels der zugelassenen beteiligten Leistungserbringer. Sie hat die Leistungserbringer bei der Erfüllung dieser Aufgabe lediglich zu unterstützen. Soweit die von der Klägerin vertraglich vereinbarten Massnahmen als zulässige Unterstützungsleistungen in Betracht kommen, darf die Klägerin hierfür nicht private Dritte einschalten. Bei diesen auf eine bessere Versorgung der Versicherten gerichteten Beratungs- und Hilfeleistungen handelt es sich um eigene Kernaufgaben, die sie nicht auf Dritte übertragen darf. Die unzulässige Einbeziehung privater Dritter in das Versorgungsmanagement bewirkt zugleich einen Verstoss gegen nationales Recht zum Schutz der Sozialdaten der Versicherten. **Krankenkassen dürfen Sozialdaten nur für gesetzeskonforme, abschliessend benannte Zwecke der gesetzlichen Krankenversicherung erheben und speichern, verarbeiten und nutzen,** nicht aber für ein gesetzeswidriges Versorgungsmanagement. Dies gilt auch bei Einbeziehung der Datenschutzgrundverordnung.»

(Hervorhebungen nicht im Original)

Quelle: Pressemitteilung Nr. 49/2029 vom 8. Oktober 2019

E. Bundesfinanzhof

a. Beschluss vom 29. August 2019, X S 6/19 – Akteneinsichtsrecht, Finanzverfahren

Kein Akteneinsichtsrecht nach DSGVO im gerichtlichen Verfahren

Nach den Leitsätzen des Beschlusses scheidet eine Akteneinsicht nach § 78 der Finanzgerichtsordnung (FGO) bei einer unzulässigen Anhörungsrüge aus; darüberhinausgehende Rechte, insbesondere auf **Akteneinsicht**, können **im gerichtlichen Verfahren nicht aus Art. 15 DSGVO hergeleitet** werden.

b. Beschluss vom 7. April 2020, II B 82/19 – Nichtanwendung DSGVO bei Steuer-fahndung

Nichtanwendbarkeit der DSGVO in Angelegenheiten der Steuerfahndung

Dazu führte der Bundesfinanzhof näher aus, dass das Finanzamt gemäss § 1 Nr. 25 der baden-württembergischen Finanzämter-Zuständigkeitsverordnung vom 30.11.2004 (LGBl. 2004, 865) im Rahmen seiner Zuständigkeit u.a. für die Aufgaben der Steuerfahndung nach § 208 AO für das FA A tätig geworden ist, und zwar im konkreten Fall nach § 208 Abs. 1 Satz 1 Nr. 1 AO ("die Erforschung von Steuerstraftaten und Steuerordnungswidrigkeiten"). Diese Tätigkeit gehört zu den Aufgaben i.S.v. Art. 2 Abs. 2 Buchst. d DSGVO. **Datenschutzrechtliche Begehren gegen das Finanzamt** im Zusammenhang mit einer Tätigkeit **betreffend die Erforschung von Steuerstrafdaten und Steuerordnungswidrigkeiten** können **in der DSGVO** daher **keine Grundlage** haben. (Rz 15)

Die Steuerfahndung kann zwar auch als Steuerermittlungsbehörde tätig werden und besitzt insoweit eine Doppelfunktion. Wenn aber gegen einen Betroffenen ein Verfahren gemäss § 208 Abs. 1 Satz 1 Nr. 1 AO eingeleitet (und noch nicht abgeschlossen) wurde, wird die Steuer-

fahndung auch in diesem Verfahren tätig, selbst wenn sie in diesem Zusammenhang Besteuerungsgrundlagen ermittelt (Rz 16, mit weiteren Nachweisen).

F. Bundesarbeitsgericht

a. Beschluss vom 7. Mai 2019, 1 ABR 53/17 – Einsichtsrecht Betriebsrat in Bruttoentgeltlisten

Keine Einschränkung des Betriebsrats-Einsichtsrechts auf anonymisierte Listen

Die Berechtigung des Betriebsausschusses oder eines nach § 28 BetrVG gebildeten Aus-schusses gemäss § 80 Abs. 2 Satz 2 Halbs. 2 BetrVG, in die Listen über die Bruttolöhne und -gehälter Einblick zu nehmen, ist nicht auf anonymisierte Listen beschränkt. (Leitsatz)

Dazu führte das Bundesarbeitsgericht näher aus (Rz 29), dass der **Einsicht in die bei der Arbeitgeberin vorhandenen Listen** mit namentlicher Nennung der Arbeitnehmenden als BezieherInnen des jeweiligen Bruttoentgelts die **DSGVO nicht entgegenstehe**.

Auf Grundlage von § 26 Abs. 1 Satz 1 des deutschen Bundesdatenschutzgesetzes (BDSG) dürfen personenbezogene Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses u.a. dann verarbeitet werden, wenn dies zur Ausübung der Erfüllung der sich aus einem Gesetz ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist (Rz 39).

Des Weiteren folgt auch beim Einsichtsrecht in Bruttoentgeltlisten die Rechtfertigung eines Eingriffs aus der inhaltlichen Ausgestaltung der entsprechenden kollektivrechtlichen Verpflichtung des Arbeitgebers (Rz 44).

III. ÖSTERREICH

A. Verfassungsgerichtshof (VfGH)

a. Erkenntnis des VfGH vom 4. März 2021, E 4037/2020 – Auskunftsrecht, Meinungsäusserungs- und Informationsfreiheit, Journalismus

Das Interesse der Öffentlichkeit an Information kann unter bestimmten Voraussetzungen persönliche Geheimhaltungsinteressen überwiegen.

Der Nationalrat wies das Auskunftsbegehren eines Journalisten zu Gehaltsfortzahlungen ehemaliger Abgeordneter aus Datenschutzgründen ab. Im weiteren Rechtsmittelverfahren erfolgte ebenfalls eine Abweisung durch das BVwG mit Erkenntnis vom 01. Oktober 2020, Z W274 2227645-1/3E. Im Rahmen einer Erkenntnisbeschwerde wurde der Fall schliesslich dem VfGH zur Entscheidung vorgelegt. Der VfGH befasste sich mit einer Abwägung der Grundrechte auf Datenschutz nach §1 DSG und Schutz des Privat- und Familienlebens nach Art. 8 EMRK gegen das Grundrecht auf Informationsfreiheit nach Art. 10 EMRK. In seinen Erwägungen gestand der VfGH dem Auskunftsbegehren im Rahmen der journalistischen Tätigkeit im öffentlichen Interesse ein besonderes, unter bestimmten Voraussetzungen vorliegendes Informationsrecht im Einzelfall zu, das dem Geheimhaltungsinteresse der ehemaligen Abgeordneten vorgehe.

Das Erkenntnis des BVwG wurde aufgehoben.

B. Verwaltungsgerichtshof (VwGH)

a. Beschluss des VwGH vom 7. September 2021, Ra 2020/11/0213 – Verarbeitung von Gesundheitsdaten im öffentlichen Interesse

Führerscheinbehörden dürfen Gesundheitsdaten ohne Einwilligung verarbeiten, da die Verbesserung der Strassenverkehrssicherheit ein erhebliches öffentliches Interesse ist.

Bei der Begründung seiner Revision brachte der Revisionswerber vor, dass die Führerscheinbehörde Gesundheitsdaten und damit personenbezogene Daten besonderer Kategorie nach Art. 9 Abs 1 DSGVO ohne seine Einwilligung, folglich unzulässig verarbeitet habe.

Der VwGH verweist auf die zulässige Verarbeitung personenbezogener Daten gemäss Art. 6 Abs. 1 Bst. e DSGVO, wenn diese zur Erfüllung einer Aufgabe im öffentlichen Interesse erforderlich ist. Auch Gesundheitsdaten dürfen nach Art. 9 Abs. 1 Bst. g DSGVO auf Grundlage der Gesetze für erhebliche öffentliche Interessen ohne Einwilligung verarbeitet werden.

Die Verbesserung der Strassenverkehrssicherheit wurde vom EuGH bereits als Ziel im allgemeinen Interesse anerkannt, damit liegt eine Aufgabe im erheblichen öffentlichen Interesse vor, die eine Einwilligung erübrigt.

Die Revision wurde zurückgewiesen.

b. Erkenntnis des VwGH vom 14. Dezember 2021, Ro 2021/04/0007 – Parteiaffinität als besonders sensibles personenbezogenes Datum

Auch eine nur mit Wahrscheinlichkeit berechnete Parteiaffinität stellt ein personenbezogenes Datum besonderer Kategorie gemäss Art. 9 Abs. 1 DSGVO dar.

Ein Unternehmen errechnete mithilfe soziodemografischer Daten die Wahrscheinlichkeit, dass sich konkrete Personen für Werbung bestimmter politischer Parteien interessierten und ordnete ihnen darauf basierend eine Parteiaffinität zu, um diese im Wege des Direktmarketing zu nutzen.

Die Verarbeitung der Parteiaffinität wurde von der österreichischen Datenschutzbehörde (DSB) per Bescheid untersagt, mit der Begründung, es handle sich um ein personenbezogenes Datum besonderer Kategorie. Das BVwG bestätigte den Bescheid der DSB und führte aus, dass die Parteiaffinität, auch wenn sie sich aus Wahrscheinlichkeiten ergeben hätte, durch die Zurechnung zu einer namentlich genannten, identifizierbaren Person dieser Person eine vermutete Nähe zur Partei unterstellen und damit den Schutzzweck nach Art. 9 Abs. 1 DSGVO berühren würde. Da sich das Unternehmen auf keine der Ausnahmebestimmungen des Art. 9 Abs. 2 DSGVO berufen konnte, insbesondere auch keine Einwilligung für die Verarbeitung durch die Betroffenen vorlag, war die Verarbeitung dieser Daten rechtswidrig.

Im Revisionsverfahren schloss sich der VwGH der Begründung des BVwG an und betonte den weiten Begriff der personenbezogenen Daten nach der DSGVO, der auch Wahrscheinlichkeitsangaben unabhängig vom Wahrheitsgehalt einen Personenbezug einräume. Diese Vermutungen seien in der Lage, ebenso negative Folgen auszulösen wie die in Art. 9 Abs. 1 DSGVO genannten tatsächlichen politischen Einstellungen. Dadurch, dass sich die Auslegung des BVwG in Einklang mit bestehender EuGH-Rechtsprechung befinde und das Unionsrecht keinen Raum für Zweifel lasse, brauche es keine Anrufung des EuGH, es handle sich um einen acte-clair.

Die Revision wurde abgewiesen, das Erkenntnis des BVwG ist rechtskräftig.

c. Erkenntnis des VwGH vom 19. Oktober 2022, Ro 2022/04/0001 – Geheimhaltungsverletzung in der Vergangenheit

Auch eine Geheimhaltungsverletzung in der Vergangenheit, welche nicht mehr fortbesteht, kann von einer Datenschutzbehörde formell festgestellt werden.

In dieser Entscheidung befasste sich der VwGH mit der Frage der – von der Revisionswerberin bestrittenen, von der österreichischen Datenschutzbehörde (DSB) und vom BVwG (Erkenntnis vom 15.10.2021, Zl. W211 2233706-1) jedoch bejahten – Zuständigkeit der DSB für die Feststellung von in der Vergangenheit liegenden Verletzungen des Rechts auf Geheimhaltung.

Bei den subjektiven Datenschutzrechten ist dabei zwischen solchen, die auf eine Leistung (insbesondere Auskunftserteilung, Löschung oder Berichtigung) abzielen – hier kann eine Klaglosstellung gemäss § 24 Abs. 6 DSG erfolgen – und dem Recht auf Geheimhaltung zu unterscheiden. «Das Recht auf Geheimhaltung verkörpert aber kein Recht auf eine bestimmte Leistung, und die Geltendmachung einer Verletzung im Recht auf Geheimhaltung ist nicht auf eine Handlung des Verantwortlichen ausgerichtet. Eine erfolgte Verletzung durch unzulässige Ermittlung kann auch nicht durch eine Handlung (im vorliegenden Fall die Löschung der betreffenden Daten) gleichsam rückwirkend wieder beseitigt werden und unterscheidet sich damit von den datenschutzrechtlich gewährleisteten Rechten, denen durch eine bestimmte Leistung entsprochen werden kann.» (Erkenntnis, Rz. 27)

Die DSB ist daher im Beschwerdeverfahren dafür zuständig, auch eine in der Vergangenheit liegende, bereits beendete Verletzung des Geheimhaltungsrechts zu untersuchen und die Rechtsverletzung durch Bescheid festzustellen.

Die Revision wurde als unbegründet abgewiesen.

C. Bundesverwaltungsgericht (BVwG)

a. Erkenntnis des BVwG vom 25. November 2019, W211 2210485-1/10E – Videoüberwachung, keine Öffnungsklausel in DSGVO

Nichtanwendung unionsrechtswidriger nationaler Datenschutzbestimmungen

Der Betreiber eines Kebab-Imbisses wurde wegen der Installation eines Videoüberwachungssystems, das Bereiche ausserhalb seines Verfügungsbereiches filmte, polizeilich angezeigt. Von der Videoaufnahme erfasst waren bspw. eine benachbarte Tankstelle sowie Teile der angrenzenden Bundesstrasse. Es fehlten zudem Hinweisschilder und die Aufzeichnungen sollten 14 Tage gespeichert bleiben.

Die österreichische Datenschutzbehörde (DSB) verhängte eine Geldbusse wegen des Filmens von Fremdgrund und der unverhältnismässigen Speicherdauer und fehlenden Kennzeichnung. Das BVwG bestätigte dem Grunde nach die Entscheidung der DSB, reduzierte die Geldbusse jedoch auf die Hälfte. Zudem führte das BVwG aus, dass die von der DSB heran-gezogenen **Bestimmungen des österreichischen Datenschutzgesetzes** (im Konkreten § 13 Abs. 3 und 5 DSG) nach der – über den Einzelfall hinausreichenden – Rechtsansicht des BVwG **unangewendet bleiben** müssen, weil sie **mangels entsprechender Öffnungsklauseln in der DSGVO** als **nicht unionsrechtskonform** anzusehen sind. Das BVwG stützte seine Erkenntnis schliesslich auf Art. 5 Abs. 1 Bst. e sowie Art. 6 Abs. 1 Bst. f DSGVO betreffend die (unverhältnismässige) Speicherdauer und Art. 5 Abs. 1 Bst. a i.V.m. Art. 12 und 13 DSGVO.

Quelle: Newsletter 2020/1 der österreichischen Datenschutzbehörde

b. Erkenntnis des BVwG vom 2. März 2020, W211 2217212-1/9E – kein Vorrang von Verwarnung gegenüber Geldbusse

Kein Vorrang von Verwarnung gegenüber Geldbusse

§ 11 des österreichischen Datenschutzgesetzes sieht vor, dass «(i)*nsbesondere bei erstmaligen Verstössen* (…) *die Datenschutzbehörde im Einklang mit Art. 58 DSGVO von ihren Abhilfebefugnissen insbesondere durch Verwarnen Gebrauch machen* (wird).»

Das BVwG hat in der gegenständlichen Entscheidung klargestellt, dass es an einer entsprechenden Öffnungsklausel in der DSGVO fehlt, die einen Vorrang des Vorgehens nach § 11 öDSG und eine Bindung der Verwaltungsbehörden und Gerichte über die DSGVO hinaus gestattet. Ein Vorrang der Verwarnung bei erstmaligen Verstössen ist mit der Systematik und dem Anwendungsvorrang der DSGVO nicht vereinbar.

Zwar gilt das Prinzip der Verhältnismässigkeit, das bereits in Art. 83 DSGVO festgelegt wird. Bei schwerwiegenden Erstverstössen kommt eine Verwarnung jedoch nicht in Betracht.

Im Ausgangsfall wurde wegen der Videoüberwachung über zwei an der Vorder- und Rückseite eines Kraftfahrzeugs angebrachten Kameras (Dash-Cams) und der damit einhergehenden rechtsgrundlosen Verarbeitung personenbezogener Daten von der österreichischen Datenschutzbehörde gegen den Fahrzeuglenker als Verantwortlichen eine Geldbusse erlassen.

Quelle: Newsletter 2020/2 der österreichischen Datenschutzbehörde

(*Anmerkung*: Vgl. dazu auch Beschluss des BVwG vom 20. November 2019, W256 2214855-1/6E)

c. Erkenntnis des BVwG vom 29. April 2020, W274 2228071-1/6E – Exzessive Beschwerdeführung

Ablehnung einer Beschwerde wegen exzessiver Beschwerdeführung

Es besteht zwar eine grundsätzliche Verpflichtung der Datenschutzbehörde sich mit Beschwerden gemäss Art. 57 Abs. 1 Bst. f DSGVO zu befassen. Die **Behandlung einer Beschwerde** kann jedoch **abgelehnt** werden, **wenn** sie **offensichtlich unbegründet oder exzessiv** (bspw. bei häufiger Wiederholung; wie im Ausgangsfall 90 Beschwerden sei Juni 2018) erfolgt.

«Ablehnung bedeutet diesfalls, dass die DSB keine inhaltliche Beurteilung der Beschwerde vornimmt, sondern die Behandlung von einer solchen Prüfung ablehnt.»

Fallgegenständlich wurde vom Beschwerdeführenden nicht aufgezeigt, dass der von ihm der Beschwerde zugrunde gelegte Sachverhalt «so individuell wäre, dass trotz der hohen Anzahl von Beschwerden» deren Behandlung berechtigt wäre.

Quelle: Newsletter 2020/3 der österreichischen Datenschutzbehörde

d. Erkenntnis des BVwG vom 28. Mai 2020, W274 2230370-1/4E – Zeugen Jehovas, Anwendbarkeit DSGVO, Auskunftsrecht

Grenzen der Anwendbarkeit von DSGVO und Auskunftsrecht

Nach Rechtsansicht des BVwG handelt es sich bei einem **verschlossenen Umschlag** (Kuvert), in der sich die Mitteilung über den Austritt aus der Glaubensgemeinschaft befindet, um **kein Dateisystem** im Sinne der DSGVO, weshalb die Anwendbarkeit der DSGVO ausgeschlossen sei.

Darüber hinaus sei das **Auskunftsrecht** nach der Judikatur des **EuGH nicht geeignet, sich Zugang zu Verwaltungsdokumenten zu sichern**. Interne Dokumente bzw. Unterlagen aus einem Ausschlussverfahren gemäss der internen Satzungen einer Glaubensgemeinschaft (fallgegenständlich der Zeugen Jehovas) seien Verwaltungsdokumenten gleichzuhalten.

Mangels genereller Anwendbarkeit der DSGVO war auf den Umfang der Datenkopie gemäss Art. 15 Abs. 3 DSGVO nicht näher einzugehen.

Quelle: Newsletter 2020/3 der österreichischen Datenschutzbehörde

e. Urteil des BVwG vom 21. Dezember 2021, W258 2238615-1 – Mitarbeiterexzess

Wenn Angestellte ohne dienstlichen Auftrag Zugriff auf eine Datenbank ihres Arbeitgebers mit personenbezogenen Daten nehmen, so gelten sie selbst als Verantwortliche.

Für die private Abfrage von Daten aus dem Zentralen Melderegister (ZMR) durch Bedienstete einer Behörde ist nicht die Behörde Verantwortlicher iSd DSG, sondern die Bediensteten.

Im Sachverhalt hatten Mitarbeitende aus Eigeninteresse Abfragen im ZMR durchgeführt. Die betroffene Person, deren personenbezogene Daten durch diese Handlungen verarbeitet wurden, erhob eine Datenschutzbeschwerde gegen die Arbeitgeberin als Verantwortliche. Da die Abfragen aber nicht für dienstliche Zwecke erfolgten und somit die Arbeitgeberin nicht Verantwortliche war, wurde die Beschwerde von der Datenschutzbehörde abgewiesen. Diese Entscheidung wurde vom BVerwG bestätigt.

Grundsätzlich sind Angestellte, die im Zuge ihrer Position in einer Organisation Zugriff zu personenbezogenen Daten haben nicht selbst Verantwortliche oder Auftragsverarbeiter iSd DSGVO. Fehlt den Angestellten aber die Berechtigung oder Zweckgebundenheit für den Zugriff auf die Daten, werden sie als Dritte bzw. selbständig Verantwortliche in Bezug auf die Datenverarbeitung eingestuft. In der Folge haften die Angestellten allein für die Verarbeitung der personenbezogenen Daten.

D. Oberster Gerichtshof (OGH)

a. Urteil des OGH vom 20. Dezember 2018, 6 Ob 131/18k – gerichtliche Geltendmachung von Löschrecht; keine Haushaltsausnahme im zivilgerichtlichen Verfahren

Im zivilgerichtlichen Verfahren kann keine Haushaltsausnahme gelten gemacht werden; die Geltendmachung des datenschutzrechtlichen Löschrechts vor Gericht ist erlaubt.

Die im Rahmen eines pflegschaftsgerichtlichen Verfahrens verwendete bzw. von der später beklagten Partei vorgelegte Korrespondenz (E-Mails) mit Angaben zur Gesundheit, Sexualleben, psychotherapeutischer Behandlung usw. der klagenden Partei unterliegt nicht dem Haushaltsprivileg, sondern diese Informationen sind als besonders sensible Daten gemäss Art. 9 i.V.m. Art. 4 Z. 2 DSGVO zu qualifizieren.

Ein auf § 77 öUrhG gestütztes Unterlassungsbegehren auf Verwendung solcher Daten im pflegschaftsgerichtlichen Verfahren schlägt – aufgrund mangelnder Wiederholungsgefahr – fehl bzw. scheitert an der Ausnahmebestimmung des § 77 Abs. 6 UrhG. Diese Ausnahme rechtfertigt die Verwendung der beanstandeten sensiblen Daten im Pflegschaftsverfahren.

Darüber hinaus bestätigte der OGH indessen das datenschutzrechtliche Löschbegehren, wonach der Beklagte die Daten unverzüglich zu löschen hat. Sie waren für jene Zwecke, für die sie erhoben wurden, nicht mehr notwendig.

Der österreichische OGH bestätigte damit, dass das in Art. 17 Abs. 1 Bst. a DSGVO vorgesehene Löschrecht im gerichtlichen Verfahren geltend gemacht werden kann, da gemäss Art. 79 Abs. 1 DSGVO jede betroffene Person unbeschadet eines verwaltungsrechtlichen oder aussergerichtlichen Rechtsbehelfs, einschliesslich des Beschwerderechts bei der Aufsichtsbehörde, das Recht auf einen wirksamen gerichtlichen Rechtsbehelf hat (siehe insb. Rz 7.1.)

b. Beschluss des OGH vom 29. August 2019, 6 Ob 152/19z – Medienprivileg, Urheberrecht

Keine schrankenlose Bildverwertung durch Zeitungen unter Berufung auf Medienprivileg

Bestimmungen des nationalen Urheberrechts – die eine zum Datenschutzrecht zwar inhaltsähnliche, aber auf den allgemeinen Persönlichkeitsschutz abstellende Schutzwirkung entfalten (in concreto § 78 des österreichischen Urheberrechtsgesetzes – UrhG) – wurden mit Inkrafttreten der DSGVO nicht materiell derogiert.

Der OGH sprach hierzu – in Anlehnung an die im Schrifttum vertretene Rechtsmeinung – aus, dass von einem Nebeneinander zwischen Urheberrechtsschutz und Datenschutz auszugehen ist (siehe 2.4) und die in § 9 Abs. 1 des österreichischen DSG vorgesehene Totalausnahme für journalistische Inhalte bzw. das Medienprivileg der DSGVO nicht jegliche Bildverwertung durch Zeitungen bzw. Medien gestatte. Mit anderen Worten: die Bildverwertung durch Zeitungen kann nicht unter Berufung auf das Medienprivileg der DSGVO schrankenlos ohne persönlichkeitsrechtliche Überlegungen bzw. ohne jegliche Interessenabwägung erfolgen.

Nach Ansicht des OGH spricht «(f)*ür die parallele Anwendung des § 78 UrhG und der DSGVO* (…), *dass § 78 UrhG primär persönlichkeitsrechtliche und nicht datenschutzrechtliche Aspekte regelt. Die Bestimmungen haben unterschiedliche Regelungsbereiche, verfolgen verschiedene Zwecke und sehen demgemäss unterschiedliche Ansprüche vor.*» (Beschluss, 3.1.)

c. Urteil des OGH vom 27. November 2019, 6 Ob 150/19f – Zivilrechtliche Abhilfemassnahme gegen Videoüberwachung

Unzulässige Videoüberwachung wegen erzeugtem ständigem Überwachungsdruck

Gegen an der Aussenfassade einer Wohnung angebrachte Überwachungskameras, die es Verantwortlichen erlauben, jederzeit Aufnahmen des eigenen Grundstücks, aber darüber hinaus auch des davor gelegenen Zugangswegs zu machen, stehen (unbenommen des Beschwerdewegs über die Datenschutzbehörde) zivilrechtliche, klagsweise geltend zu machende Abhilfemassnahmen zur Verfügung.

Durch die angebrachte Kamera entstehe ein ständiger Überwachungsdruck auf die klagende Partei, die neben Bestimmungen der DSGVO auch eine Verletzung in ihrem Grundrecht auf Privatsphäre und des Rechts am eigenen Bild bedeutet. Eine derartige Videoüberwachungsanlage bzw. Kamera fällt nicht unter das Haushaltsprivileg gemäss Art. 2 Abs. 2 Bst. c DSGVO, da sie nicht bloss zu familiären Zwecken eingesetzt wird. Wenn sie bspw. der Beweissicherung dient, greift das Haushaltsprivileg nicht. Das österreichische Datenschutzgesetz (DSG) führt in §§ 12 und 13 den Begriff der «Bildaufnahme» näher aus, der extensiv auszulegen ist. Auch die Zulässigkeitsgrenzen einer Bildaufnahme werden gesetzlich näher ausgeführt. Diese wurden gegenständlich nicht gewahrt, da der Verantwortliche, d.h. «*der Beklagte, über das unvermeidliche Ausmass hinaus einen Teil des öffentlichen Zugangswegs und* (…) *einen* (…) *Teil des privaten Gartens* (…) *des Klägers filmt*».

Das Recht auf Wahrung der Geheimsphäre – in Österreich als Teilbereich des Persönlichkeitsrechts i.S.v. § 16 ABGB verbürgt – steht einem solchen Eindringen in die Privatsphäre einer Person, wie durch die gegenständliche Videoaufnahmen ersichtlich, entgegen. Mit Verweis auf seine ständige Judikatur (6 Ob 2401/96y, 6 Ob 6/06k, 6 Ob 231/16 p und 3 Ob 195/17y) hielt der OGH fest, dass ein Überwachungsdruck zu verhindern ist, d.h. «(e)*iner Person darf nicht das Gefühl gegeben werden, dass sie jederzeit überwacht werden kann*. (…) *Entscheidend ist, ob nach den Umständen des Falls die konkrete Befürchtung* (eines objektiven, unbefangenen Betrachters) *besteht, dass die Kamera jederzeit in Betrieb gesetzt werden könnte*». (Beschluss, 7.2.2.)

Fallgegenständlich war die Überwachungsanlage im Rahmen der vorgenommenen Interessenabwägung überschiessend und das Klagebegehren auf Entfernung und künftiger Unterlassung der Anbringung einer Überwachungskamera berechtigt.

d. Urteil des OGH vom 29. August 2022, 6 Ob 198/21t – Informationsfreiheit und Datenschutz bei Bewertungsportalen

Das erhebliche Interesse der Öffentlichkeit an den Informationen im Bewertungsportal überwiegt das Interesse auf Privatsphäre, da es darin nur um die bereits öffentlich wahrnehmbare Berufsausübung geht.

Im Sachverhalt ging es um ein Internetportal, auf dem Nutzer Punktebewertungen und Erfahrungsberichte zu Ärzten abgeben konnten. Die Erstklägerin war eine Ärztin, die auf dem Internetportal auffindbar und bewertbar war. Sie verlangte die Löschung aller Daten und Bewertungen zu ihrer Person unter Berufung auf Datenschutz- und Persönlichkeitsrechte.

Der OGH nahm eine umfassende Interessenabwägung im Sinne des Art. 6 Abs. 1 lit. f DSGVO vor. Die Verarbeitung der Daten im Portal ist für die möglichst umfassende Information der Nutzer notwendig und von Meinungs- und Informationsfreiheit geschützt gemäss Art. 10 EMRK und Art. 11 GRC. Es stehen sowohl die durch die Informationsfreiheit geschützten berechtigten Nutzerinteressen als auch die von Art. 16 GRC geschützten gewerblichen eigenen Interessen der Beklagten den Interessen der Klägerin gegenüber. Das erhebliche Interesse der Öffentlichkeit an den Informationen des Portals überwiegt gemäss der Entscheidung des OGH gegenüber den Datenschutzrechten der Beklagten, zumal nur die von der Öffentlichkeit wahrnehmbare Berufsausübung betroffen ist und nicht ihre Privatsphäre. Weiters steht der Klägerin ein Beschwerdesystem zur Verfügung steht.

Der Revision wurde nicht Folge gegeben.

e. Urteil des OGH vom 23. Oktober 2023, 6 Ob 205/22y – Keine Herausgabe eines verletzenden Videos

Es kann lediglich die Löschung eines verletzenden Videos verlangt werden, nicht jedoch dessen Herausgabe.

In Rechtsprechung und Lehre ist anerkannt, dass die Verletzung von Persönlichkeitsrechten bei bereits erfolgten Verstössen neben Unterlassungsansprüchen auch Beseitigungsansprüche, die die Form eines Anspruchs auf Vernichtung annehmen können, nach sich ziehen kann. So kann dem in seinem Recht am eigenen Wort Verletzten – abhängig von der im Fall der Behauptung eigener Interessen des Eingreifers vorzunehmenden Interessenabwägung – ein Anspruch auf Löschung rechtswidrig erlangter Tonaufzeichnungen zustehen.

Hingegen kann aus der dargestellten Rechtsprechung kein aus dem Persönlichkeitsrechtseingriff folgender Anspruch auf Herausgabe von Bild- oder Tonaufnahmen abgeleitet werden.

IV. FRANKREICH

A. Conseil constitutionnel

Der «Conseil constitutionnel», zu Deutsch der französische «Verfassungssrat», ist zur Entscheidung über die Normenkontrolle, d.h. die Verfassungsmässigkeit von einfachen Gesetzen, Verfassungsergänzungsgesetzen, völkerrechtlichen Verpflichtungen sowie den Geschäftsordnungen der französischen Parlamentskammern zuständig und erfüllt demgemäss eine dem liechtensteinischen Staatsgerichtshof ähnliche Funktion eines Verfassungsgerichts in Frankreich. Seine Kompetenzen unterscheiden sich indessen von jenen des StGH.

(**Quelle: https://www.conseil-constitutionnel.fr/de**)

a. Entscheidung N° 2019-796 DC vom 27. Dezember 2019 – Unzulässigkeit automatisierter Datenverarbeitung durch die Steuerverwaltung

Grenzen automatisierter Datenverarbeitung aus öffentlichen Quellen durch Steuerbehörde

Der Verfassungsrat hob Bestimmungen des französischen Steuergesetzes (Artikel 154 Steuergesetz) auf, wonach die Steuer- und Zollverwaltungen für einen Zeitraum von drei Jahren ermächtigt wurden, personenbezogene Daten, die auf den Websites bestimmter Plattformbetreiber öffentlich zugänglich sind, zum Zwecke der Untersuchung von Steuer- und Zollvergehen und -verletzungen automatisiert zu sammeln und zu verarbeiten.

Der Verfassungsrat erkannte eine Verletzung des Rechts auf Achtung der Privatsphäre durch die gesetzliche Ermächtigung der Steuerverwaltung, computergestützte und automatisierte Mittel zu verwenden, die es ihr ermöglichten, grosse Datenmengen über öffentliche Online-Plattformen oder Kommunikationsdienste zu sammeln und diese systematisch zu verarbeiten (Aggregation, Vergleich und Analyse).

Der Verfassungsrat betonte, dass nur solche Inhalte gesammelt und verwendet werden dürfen, die sich auf jene Person beziehen, die sie absichtlich veröffentlicht hat. Dies umfasst jedoch nicht besonders schützenswerte Daten gemäss Art. 9 DSGVO.

Es obliegt der Aufsichtsbehörde, dass bei algorithmischer Auswertung der Daten nur die für die verfolgten Zwecke unbedingt erforderlichen Daten erhoben und gespeichert werden.

Der Verfassungsrat hob jene Bestimmungen auf, die eine automatische Sammlung und Nutzung von Daten zur Untersuchung einer Unterlassung oder Verzögerung der Einreichung einer Steuererklärung (also zur Ahndung einer steuerrechtlichen Übertretung) vorsahen. Die darin vorgesehene automatisierte Verarbeitung wurde für nicht notwendig und damit unverhältnismässig erachtet, da die Steuerverwaltung in strittigen Fällen bereits Kenntnis von einem Verstoss hatte.

Anzumerken ist, dass der Verfassungsrat die Aufhebung der Bestimmungen des Steuergesetzes nicht auf den durch die DSGVO gebotenen Schutz gestützt hatte, sondern vielmehr auf die allgemeinere verfassungsrechtliche Verbürgung des Schutzes der Privatsphäre.

Quelle: **Pressemitteilung vom 27. Dezember 2019**

b. Entscheidung N° 2020-800 DC vom 11. Mai 2020 – COVID-19, Verarbeitung von Gesundheitsdaten

Datenschutzkonformität eines Kontaktverfolgungs-Systems

Der französische Verfassungsrat hob diverse Bestimmungen des Gesetzes zur Ausdehnung des gesundheitlichen Notstands (zur Bekämpfung und Eindämmung der COVID-19-Pandemie) auf. Die Bestimmungen zur Verarbeitung personenbezogener Daten (Gesundheitsdaten) zum Zweck der «Rückverfolgung» wurden teilweise aufgehoben bzw. erhob der Verfassungsrat diverse Auslegungsvorbehalte.

Soweit mit den Bestimmungen ein Informationssystem eingerichtet werden soll, das zur Verarbeitung von Daten zur Rückverfolgung von Personen bestimmt ist, die von COVID-19 betroffen sind, erkannte der Verfassungsrat unter anderem eine Beeinträchtigung des Rechts auf Achtung der Privatsphäre, da die Verarbeitung solcher als Gesundheitsdaten zu qualifizierenden personenbezogenen Daten über ein ad-hoc-Informationssystem ohne Einwilligung der Betroffenen erfolgen sollte. Jedoch verfolgte sie das verfassungsrechtlich anerkannte Ziel des Gesundheitsschutzes, durch Nachverfolgung bzw. Identifikation von Ansteckungsketten.

Im Ergebnis erachtete der Verfassungsrat, trotz des besonderen Umfangs der einwilligungslos verarbeiteten Daten, dass deren Verarbeitung zum Zweck der Eindämmung der Pandemie erforderlich ist. Ein Zugriff aus anderen Gründen, die nicht direkt mit der Bekämpfung der Pandemie zusammenhängen, ist jedoch nicht gerechtfertigt.

Die vorgesehene zeitliche Begrenzung, wonach die Datenverarbeitung nicht über den zur Bekämpfung der COVID-19-Pandemie notwendigen Zeitraum hinausreicht bzw. spätestens sechs Monate nach dem Ende des ausgerufenen Notstands (vom 23. März 2020) beendet werden muss, wurde vom Verfassungsrat ebenso berücksichtigt. In Summe gelangte der Verfassungsrat zum Ergebnis, dass die Datenverarbeitung (soweit sie der Eindämmung der Pandemie diente) das Recht auf Privatsphäre nicht verletzte.

Quelle: **Pressemitteilung vom 11. Mai 2020**

c. Entscheidung N° 2020-841 QPC vom 20. Mai 2020 – «La Quadrature du Net»

Keine unbegrenzte Datenverarbeitung durch Behörde

Der Verfassungsrat hob Bestimmungen auf, die den Zugang der «HADOPI» (zu Deutsch: «Hohe Behörde für die Verbreitung von Werken und den Schutz der Rechte im Internet») zu allen Dokumenten, einschliesslich der Verbindungsdaten der Internetnutzer, regelten.

Die (aufgehobenen) Bestimmungen des französischen Urheberrechts (Art. L. 336-3) regelten, dass Inhaber einer elektronischen Kommunikationsplattform dazu verpflichtet waren, dafür zu sorgen, dass der Zugang nicht zum Zweck der Vervielfältigung, Darstellung, Bereitstellung oder öffentlichen Wiedergabe von urheberrechtlich geschützten Werken ohne Genehmigung der Urheber erfolgt. Die Kontrolle darüber war einer in der HADOPI eingerichteten Kommission vorbehalten.

Die teilweise aufgehobenen Bestimmungen sahen weitgehende Kompetenzen der Kommission vor, etwa das Recht von den Kommunikationsdienstanbietern diverse personenbezogene Daten (bspw. Identität, Postanschrift, E-Mail, Telefonnummern) sowie alle Dokumente oder Verbindungsdaten im Besitz der Plattformanbieter anzufordern.

Soweit sich der Umfang der fraglichen Informationen auf die Identität und die oben genannten Kontaktdaten von Personen beschränkt, denen ein Urheberrechtsverstoss angelastet wird, sind diese als erforderlich anzusehen, damit die Behörde ihre Aufgaben erfüllen kann. Diesbezüglich war keine Verfassungswidrigkeit zu erkennen. Die darüberhinausgehende gesetzliche Anordnung in Bezug auf alle Dokumente und Verbindungsdaten stehen jedoch nicht notwendigerweise in direktem Zusammenhang mit der Einhaltung bzw. Verstössen gegen die Vorgaben des französischen Urheberrechts. Daher war der Zugriff auf sämtliche Dokumente und Verbindungsdaten verfassungswidrig und wurde mit Wirksamkeit ab 31.12.2020 aufgehoben.

Quelle: Pressemitteilung vom 20. Mai 2020

B. Conseil d'Etat

Der Conseil d'Etat, zu Deutsch der französische «Staatsrat», erfüllt sowohl die Funktion des obersten Verwaltungsgerichts in Frankreich als auch der Beratung der Regierung in Rechtsfragen. Hinsichtlich seiner judikativen Kompetenzen ist der französische Staatsrat mit dem liechtensteinischen Verwaltungsgerichtshof (VGH) vergleichbar.

(**Quelle: https://www.conseil-etat.fr/de/**)

a. Entscheidungen N° 440442 und 440445 vom 18. Mai 2020 – Drohneneinsatz zur Personenidentifikation

Verwendung von Drohnen zur Identifikation von Personen unzulässig

Der Entscheidung des Staatsrats lag ein an das Pariser Verwaltungsgericht gerichtetes Begehren zweier Menschenrechtsorganisationen (La Quadrature du Net und der französischen Menschenrechtsliga) zugrunde, die Einstellung der Überwachung durch Drohnen anzuordnen. Diese ist von der Polizeipräfektur zur Durchsetzung der Eindämmungsmassnahmen der COVID-19-Pandemie vorgesehen worden. Das Pariser Verwaltungsgericht hatte den Antrag abgelehnt,

wogegen sich die gegenständliche Beschwerde an den Staatsrat richtete. Dieser wies im Ergebnis die unverzügliche Einstellung der genannten Drohnenüberwachung an.

Die Polizeipräfektur von Paris hatte darauf hingewiesen, dass Drohnen nicht zur Identifizierung von Personen, sondern nur zur Aufdeckung von Zusammenkünften in der Pariser Öffentlichkeit entgegen den geltenden Gesundheitsvorschriften eingesetzt werden dürfen, um solche Zusammenkünfte in der Folge aufzulösen oder Räumlichkeiten zu evakuieren. Nach Angabe der Polizeipräfektur überfliegen die Drohnen die Stadt in einer Höhe von 80 bis 100 Metern, verfügen über ein Weitwinkelobjektiv, jedoch würden mangels Speicherkarte keine Aufzeichnungen erfolgen.

Der Staatsrat stellte indessen fest, dass die eingesetzten Drohnen mit einem optischen Zoom ausgestattet sind und unterhalb von 80 Metern fliegen können, was die Erfassung von Identifikationsdaten ermöglicht. Darüber hinaus wiesen die Drohnen keinerlei technische Vorrichtungen auf, um sicherzustellen, dass die gesammelten Informationen nicht zur Identifizierung von gefilmten Personen führen können.

Es war daher eine Verarbeitung personenbezogener Daten zu erkennen. Diese entsprach nicht dem geltenden Datenschutzrecht, weshalb die unverzügliche Einstellung der Überwachung durch Drohnen angeordnet wurde, bis ein Ministerialerlass oder ein Dekret zu diesem Thema nach Konsultation der französischen Aufsichtsbehörde (CNIL) erlassen werde oder bis die Drohnen mit einer Vorrichtung ausgestattet sind, die es unmöglich macht, die gefilmten Personen zu identifizieren.

Quelle: **«Le Conseil d'État ordonne à l'État de cesser immédiatement la surveillance par drone du respect des règles sanitaires»** (Website des Conseil d'Etat)

b. Entscheidung N° 430810 vom 19. Juni 2020 – Geldbusse CNIL gegen Google

Anforderungen an eine gültige Einwilligung und Informationspflichten

Der Staatsrat bestätigte die von der französischen Datenschutzaufsichtsbehörde (CNIL) verhängte Geldbusse gegen Google wegen Nichteinhaltung der Anforderungen der DSGVO. Die verhängte Geldbusse in der Höhe von EUR 50 Millionen ist nicht unverhältnismässig. Google hatte den Nutzern von Android-Systemen keine ausreichend klaren und transparenten Informationen zur Verfügung gestellt und sie daher nicht in die Lage versetzt, eine verbindliche Einwilligung zur Verarbeitung ihrer personenbezogenen Daten zum Zweck der Personalisierung von Werbung zu geben.

Der Staatsrat präzisierte folglich die Pflichten der Verantwortlichen für die Verarbeitung personenbezogener Daten in Bezug auf Information und Einholung einer Einwilligung.

Der Staatsrat stellte fest, dass ein Nutzer, der ein Google-Konto für die Nutzung des Android-Systems einrichten möchte, zunächst aufgefordert wird, der Verarbeitung seiner Daten gemäss einer Standardeinstellung (einschliesslich Personalisierungsfunktionen für Werbung) zuzustimmen. Die zu diesem Zeitpunkt zur Verfügung gestellten Informationen über Ad Targeting sind allgemein und «verwässert», sie stehen inmitten von Informationen über andere Zwecke.

Während die Einholung der Einwilligung auf dieser Ebene global für alle von der Daten-verarbeitung verfolgten Zwecke erfolgt, bestätigt der Staatsrat die Einschätzung der CNIL, dass die Informationen über die gezielte Werbung nicht klar und deutlich genug dargestellt werden, um die Einwilligung des Nutzers gültig zu erfassen.

Der Staatsrat stellte des Weiteren fest, dass der Nutzer zwar durch Klicken auf einen Link "weitere Optionen" zusätzliche Informationen über die gezielte Werbung erhalten kann und dann gebeten wird, seine ausdrückliche Zustimmung zu diesem Zweck zu erteilen. Diesbezüglich ist der Staatsrat aber der Ansicht, dass auch die auf dieser zweiten Ebene von Google bereitgestellten Informationen unzureichend sind. Darüber hinaus wird dort die Einwilligung mittels eines vorangekreuzten Kästchens eingeholt, was ebenfalls nicht den Anforderungen der DSGVO entspricht.

Quelle: **«RGPD: le Conseil d'État rejette le recours dirigé contre la sanction de 50 millions d'euros infligée à Google par la CNIL»** (Website des Conseil d'Etat)

c. Entscheidung N° 434684 vom 19. Juni 2020 – Cookie-Walls

Unzulässigkeit allgemeiner und absoluter Verbote von Cookie-Walls aufgrund von Leitlinien (soft-law) der Datenschutzbehörde

Die französische Datenschutzbehörde (CNIL) hatte nach Inkrafttreten der DSGVO neue Richtlinien zu «Cookies» und anderen Tracing-Werkzeugen verabschiedet; darin war unter anderem ein allgemeines Verbot der Verwendung sogenannter «Cookie-Walls» vorgesehen. Darunter sind technische Vorrichtungen zu verstehen, die dazu dienen, den Zugang zu einer Website zu blockieren, wenn Cookies abgelehnt werden.

Der Staatsrat entschied, dass ein derartiges allgemeines Verbot im Wege von Richtlinien der CNIL nicht zulässig ist. Darüber hinaus bestätigte der Staatsrat jedoch die Rechtmässigkeit anderer strittiger Punkte in Bezug auf die Erfassung der Zustimmung von Internetnutzern betreffend Cookies und anderer «Tracing»-Werkzeuge.

Die CNIL kann auf Grundlage der DSGVO keine allgemeine Leitlinie bzw. Richtlinien erlassen, die ein Verbot von «Cookie-Walls» vorsieht. Nach Rechtsansicht des französischen Staatsrates könne die CNIL unter dem Deckmantel von soft-law-Regelungen keine allgemeinen und absoluten Verbote aussprechen.

Quelle: **«Le Conseil d'État annule partiellement les lignes directrices de la CNIL relatives aux cookies et autres traceurs de connexion»** (Website des Conseil d'Etat)

d. Entscheidung N° 440916 vom 19. Juni 2020 – COVID 19, Gesundheitsdaten

Zulässigkeitsvoraussetzungen für Plattform zum Management von Gesundheitsnotfällen

Der Entscheidung des Staatsrats liegt das Begehren verschiedener Organisationen und Verbände zugrunde, einen Regierungserlass bzw. ein Dekret («l'arrêté») vom 21. April 2020

aufzuheben, mit dem die Plattform «*Health Data Hub*» ermächtigt wurde, diverse Gesundheitsdaten für das Management von Gesundheitsnotfällen zu sammeln.

Insbesondere wurden von den Beschwerdeführenden die Modalitäten für das Hosting der Daten, ihre (fehlende) Anonymisierung, die Möglichkeit zur Übertragung in Drittländer und die Sicherheit der Plattform beanstandet.

Der Staatsrat führte in seiner Entscheidung aus, dass der Gesundheitsminister die Plattform dazu ermächtigt hatte, pseudonymisierte Gesundheitsdaten zu sammeln und zu verarbeiten, die zur Verfolgung von Projekten von öffentlichem Interesse im Zusammenhang mit der COVID-19-Pandemie – ausschliesslich während des Gesundheitsnotstandes – erforderlich sind. Zur Rechtfertigung des Rückgriffs auf die Plattform müssen folgende Kriterien erfüllt sein:

- Dringlichkeit des Projekts;
- Fehlen einer zufriedenstellenden technischen Alternative, die rechtzeitig umgesetzt werden kann, und
- Autorisierung durch die französische Aufsichtsbehörde (CNIL).

Unter diesen Umständen erkannte der Staatsrat, dass die im Ministerialerlass vorgesehene Datenerhebung legitime Zwecke verfolgte und zur Erreichung dieser Ziele verhältnismässig war.

In Bezug auf die Datensicherheit der Plattform führte der Staatsrat aus, dass der Host (Microsoft) die Daten in Europa speichert (derzeit in den Niederlanden und demnächst in Frankreich). Die Verarbeitung erfolge in Rechenzentren, die von der Zertifizierung als "Gesundheitsdaten-Host" gemäss dem Gesetz über das öffentliche Gesundheitswesen profitieren. Der Staatsrat stellte fest, dass Microsoft gemäss dem von ihm unterzeichneten Vertrag den Anforderungen der französischen Vorschriften über das Hosting von Gesundheitsdaten unterliegt und die DSGVO in Bezug auf die Übermittlung personenbezogener Daten in Drittstaaten (insbesondere hinsichtlich des möglichen Datentransfers in die Vereinigten Staaten) einhalten muss. (*Anmerkung: der Staatsrat stellt hierzu noch auf den wenig später durch den EuGH für ungültig erklärten Privacy-Shield-Durchführungsbeschluss ab*).

In Bezug auf die Pseudonymisierung der Daten wurde vom Staatsrat angeordnet, dass die Plattform der CNIL innerhalb von fünf Tagen alle Elemente im Zusammenhang mit den verwendeten Pseudonymisierungsverfahren mitteilen muss, damit sie diese überprüfen kann.

Schliesslich wurde festgestellt, dass die von der Plattform bereitgestellten Informationen über die gesammelten Daten unvollständig seien. Der Staatsrat forderte die Plattformbetreiber daher auf, auf ihrer Website bestimmte Klarstellungen bezüglich der möglichen Übermittlung von Daten ausserhalb der Europäischen Union sowie Informationen über die Rechte der betroffenen Personen bereitzustellen.

Quelle: **«Plateforme Health Data Hub»** (Website des Conseil d'Etat)

e. Entscheidung N° 441065 vom 26. Juni 2020 – Verwendung von Wärmebildkameras zur Bekämpfung von COVID-19

Unzulässige Verwendung von Wärmebildkameras bei Schulen

Der Staatsrat ordnete anlässlich der Beschwerde der französischen Menschenrechtsliga die verantwortliche Gemeinde Lisses an, die Verwendung von Wärmebildkameras in der Nähe von Schulen, die zur Eindämmung der COVID-19-Pandemie vorrübergehend installiert worden waren, einzustellen. Die Gemeinde hatte die Verwendung von Wärmebildkameras zur Temperaturmessung vorgesehen.

Die Verwendung dieser Wärmebildkameras stellt – im Gegensatz zu solchen, die an städtischen Gebäuden fest installiert sind – eine Verletzung des Rechts auf Achtung der Privatsphäre sowohl der SchülerInnen als auch des Lehrpersonals dar. Der Unterschied sei nach Ansicht des Staatsrats darin zu erkennen, dass SchülerInnen und Lehrpersonal sich dieser Temperaturmessung zwingend unterwerfen müssen, während beim Zugang zu Amtsgebäuden Wahlfreiheit hierüber bestehe.

Entgegen der Behauptung der Gemeinde, dass die Verarbeitung auch auf einer Einwilligung im Sinne von Art. 9 Abs. 2 Bst. a der DSGVO beruhe, erkannte der Staatsrat keinen Grund, davon auszugehen, dass diese Zustimmung den Anforderungen von Art. 7 DSGVO und, soweit Kinder betroffen sind, den zusätzlichen Anforderungen von Art. 8 DSGVO entspricht. Obwohl die Stadtverwaltung behauptet, jeder Familie ein Einwilligungsformular geschickt zu haben, konnte sie weder nachweisen, dass diese Zustimmung tatsächlich vor der Inbetriebnahme der Kameras für jedes Kind eingeholt wurde, noch dass sie speziell für diese Datenverarbeitung erteilt wurde und alle notwendigen Informationen enthält, insbesondere hinsichtlich der Ausübung des Rechts auf Auskunft, Berichtigung, eventuellen Widerspruch oder die Möglichkeit, diese Einwilligung zu widerrufen. Die Tatsache, dass der Zugang der Kinder zur Schule an die Bedingung geknüpft war, dass die Verwendung der Temperaturmessung mittels Wärmekamera akzeptiert wird, schliesst in jedem Fall die Möglichkeit einer freiwilligen Zustimmung aus.

Quelle: **«Caméras thermiques à Lisses: le juge des référés ordonne de mettre fin à leur usage dans les écoles»** (Website des Conseil d'Etat)

f. Entscheidung N° 444937 vom 13. Oktober 2020 – Folgen von Schrems II auf Health Data Hub

Kein Verbot der nationalen Gesundheitsdatenbank (Health Data Hub)

Der Staatsrat hatte sich mit der Beschwerde diverser Verbände auseinanderzusetzen, die forderten, dass die Gesundheitsplattform «Health Data Hub» ausgesetzt werde. Im Rahmen eines Auftragsverarbeitungsvertrags würden personenbezogene Daten über Microsoft (in den Niederlanden) gehostet. Die Übermittlung dieser Daten ausserhalb der Europäischen Union ist auf Grundlage dieses Auftragsverarbeitungsvertrags nicht zulässig. Die Plattform wurde jedoch – trotz des Risikos der Übermittlung von personenbezogenen Daten in die Vereinigten Staaten – nicht deaktiviert. Vielmehr ist es erforderlich besondere Vorsichtsmassnahmen unter Aufsicht der CNIL vorzunehmen.

«Health Data Hub» (siehe bereits oben Punkt B.d.) wurde als öffentliche Datenbank im November 2019 eingerichtet, um den Austausch von Gesundheitsdaten zu Forschungszwecken zu erleichtern. Einige dieser Daten werden nun zur Eindämmung der COVID-19-Pandemie verwendet. Im April 2020 wurde ein Auftragsverarbeitungsvertrag zwischen der Plattform und einer irischen Tochtergesellschaft von Microsoft betreffend das Hosting der Daten und die Nutzung der für die Verarbeitung notwendigen Software geschlossen.

In Folge des «Schrems II»-Urteils (C-311/18) des EuGH, mit dem der «Privacy-Shield»-Angemessenheitsbeschluss ungültig erklärt wurde, beantragten mehrere Verbände die Aussetzung der Verarbeitungstätigkeit durch die Health Data Hub.

In der Verarbeitung personenbezogener Daten durch Microsoft (bzw. ein Tochterunternehmen) im Gebiet der Europäischen Union (des EWR) ist per se keine schwerwiegende oder offenkundige Rechtswidrigkeit zu erkennen. Der Staatsrat kann zwar nicht zur Gänze ausschliessen, dass U.S.-Behörden um Zugriff auf Daten von Microsoft, respektive ihrer irischen Niederlassung ersuchen. Ein DSGVO-Verstoss wäre jedoch rein hypothetisch, da nach Ansicht des Staatsrats nicht auszuschliessen ist, dass Microsoft sich nicht gegen einen solchen behördlichen Datenzugriff zur Wehr setzt. Abseits davon, ist ein wichtiges öffentliches Interesse an der Nutzung der Gesundheitsdaten (und folglich deren Verarbeitung durch die zur Verfügung stehenden technischen Mittel) in der Eindämmung der COVID-19-Pandemie zu erkennen.

Angesichts des erkannten Risikos wurde die Gesundheitsplattform ersucht, ihre bisherigen Sicherheitsvorkehrungen zu verschärfen und unter Aufsicht der französischen Datenschutz-behörde (CNIL) weiter mit Microsoft zusammenzuarbeiten. Der Staatsrat betonte, dass es sich dabei um eine bloss vorübergehende Anordnung handelt. Die Vorkehrungen müssen getroffen werden, bis eine nachhaltige Lösung gefunden werde, die jegliche Zugriffsrisiken durch U.S.-Behörden ausschliessen.

Quelle: **«Health Data Hub et protection de données personnelles : des précautions doivent être prises dans l'attente d'une solution pérenne»** (Website des Conseil d'Etat)

V. EUROPÄISCHE UNION

A. Europäischer Gerichtshof (EuGH)

a. Urteil des EuGH vom 14. Februar 2019, Nr. C-345/17 (Buivids) – Grenze des Haushaltsprivilegs

Das Haushaltsprivileg greift nicht mehr, wenn Videos auf Social Media Plattformen wie YouTube hochgeladen und dort unbeschränkt veröffentlicht werden. Die Zugänglichmachung der Aufnahmen für eine unbestimmte Anzahl an Personen spricht gegen einen rein persönlichen oder familiären Beweggrund der Verarbeitung.

Der EuGH hat entschieden, dass auch das Hochladen und Veröffentlichen von personenbezogenen Daten auf einer Webseite, z.B. auf einer Social Media Plattform, eine ganz oder teilweise automatisierte Verarbeitung dieser Daten darstellt. Wird die Veröffentlichung z.B. eines Videos ausserdem ohne Zugangsbeschränkung vorgenommen und die personenbezogenen Daten somit einer unbestimmten Anzahl von Personen über das Internet zugänglich gemacht, so handelt es sich auch nicht mehr um eine Verarbeitung im Rahmen der Ausübung ausschliesslich persönlicher oder familiärer Tätigkeiten (Haushaltsprivileg, Haushaltsausnahme), sondern die Bestimmungen der DSGVO kommen vollständig zur Anwendung.

b. Urteil des EuGH vom 12. Januar 2023, Nr. C-154/21 (Österreichische Post) – Auskunftsrecht über die Empfänger personenbezogener Daten

Eine betroffene Person hat das Recht, Auskunft über die konkreten Empfänger ihrer Daten zu erhalten, um die Betroffenenrechte aus Art. 16, 17, 18 DSGVO wahrnehmen zu können.

Der EuGH hat entschieden, dass der Auskunftsanspruch aus Art. 15 Abs. 1 Bst. c DSGVO regelmässig auch die Identität der Empfänger personenbezogener Daten umfasst. Nur wenn es (noch) nicht möglich ist, diese Empfänger zu identifizieren, kann sich der Verantwortliche darauf beschränken, lediglich die Kategorien der betreffenden Empfänger mitzuteilen. Dies ist ebenfalls der Fall, wenn der Verantwortliche nachweist, dass der Antrag offenkundig unbegründet oder exzessiv im Sinne von Art. 12 Abs. 5 DSGVO ist.

c. Urteil des EuGH vom 4. Mai 2023, Nr. C-487/21 (Österreichische Datenschutzbehörde und CRIF) – Auskunftsrecht, Recht auf Kopie

Das Recht auf Kopie reicht soweit, wie eine solche unerlässlich ist, um der betroffenen Person die wirksame Ausübung ihrer Rechte nach DSGVO zu ermöglichen

Der EuGH stellt fest, dass das Recht auf Kopie nach Art. 15 Abs. 3 DSGVO die originalgetreue und verständliche Reproduktion der personenbezogenen Daten des Betroffenen umfasst. Dieses Recht setzt das Recht voraus, eine Kopie von Auszügen aus Dokumenten oder gar von ganzen Dokumenten oder auch von Auszügen aus Datenbanken, die u. a. diese Daten

enthalten, zu erlangen, wenn die Zurverfügungstellung einer solchen Kopie unerlässlich ist, um der betroffenen Person die wirksame Ausübung der ihr durch diese Verordnung verliehenen Rechte zu ermöglichen, wobei insoweit die Rechte und Freiheiten anderer zu berücksichtigen sind.

Art. 15 Abs. 3 Satz 3 DSGVO ist dahin auszulegen, dass sich der im Sinne dieser Bestimmung verwendete Begriff «Informationen» ausschliesslich auf personenbezogene Daten bezieht, von denen der für die Verarbeitung Verantwortliche gemäss Satz 1 dieses Absatzes eine Kopie zur Verfügung stellen muss.

d. Urteil des EuGH vom 4. Mai 2023, Nr. C-300/21 (Österreichische Post) – Recht auf Schadenersatz

Voraussetzung für einen Schadenersatzanspruch ist, dass ein Schaden eingetreten ist, der kausal auf einem Verstoss gegen die DSGVO beruht. Eine Erheblichkeitsschwelle gibt es dabei nicht.

In einem weiteren Urteil hat sich der EuGH mit dem Recht auf Schadenersatz nach Art. 82 DSGVO auseinandergesetzt. Der EuGH betont, dass die Begriffe des materiellen und immateriellen Schadenersatzes als autonome Begriffe des Europarechts in allen Mitgliedsstaaten einheitlich auszulegen sind. Voraussetzung für einen Schadenersatzanspruch ist, dass ein Schaden eingetreten ist, der kausal auf einem Verstoss gegen die DSGVO beruht. Daraus folgt, dass nicht jeder Verstoss gegen die DSGVO automatisch zu einem Schadenersatzanspruch führt.

Eine Erheblichkeitsschwelle, so der EuGH, muss nicht erreicht werden, um Anspruch auf einen immateriellen Schadenersatz zu haben. In der DSGVO wird ein solches Erfordernis nicht erwähnt und eine solche Beschränkung stünde zu dem vom Unionsgesetzgeber gewählten weiten Verständnis des Begriffs «Schaden» im Widerspruch.

Zu den Regeln für die Bemessung des Schadenersatzes stellt der EuGH fest, dass Art. 82 DSGVO dahin auszulegen ist, dass es die Aufgabe der einzelnen Mitgliedstaaten ist, die Modalitäten festzulegen. Hierbei sind jedoch die unionsrechtlichen Grundsätze der Äquivalenz und der Effektivität zu beachten.

e. Urteil des EuGH vom 4. Juli 2023, Nr. C-252/21 (Meta v. Bundeskartellamt) – Einwilligung; Vertragserfüllung; rechtliche Verpflichtung; berechtigtes Interesse; besondere Kategorien personenbezogener Daten; DSGVO und Wettbewerbsrecht

Eine rechtmässige Einwilligung setzt eine echte Wahlmöglichkeit und bewusste Entscheidung voraus, was nicht mittels AGB als Vertragsbestandteil umgangen werden kann. Die Marktstellung eines Betreibers ist ein wichtiger Aspekt bei der Prüfung der Freiwilligkeit einer Einwilligung. Die Erforderlichkeit der Rechtsgrundlagen gemäss Art. 6 Abs. 1 Bst. b – f DSGVO ist eng auszulegen. Sensible Daten gelten nur dann als offensichtlich öffentlich gemacht, wenn zuvor explizit die Entscheidung zum Ausdruck gebracht wird, die

betreffenden Daten einer unbegrenzten Zahl von Personen öffentlich zugänglich zu machen. Es gilt der Grundsatz der loyalen Zusammenarbeit zwischen Wettbewerbs- und Datenschutzaufsichtsbehörden.

In Frage stand gegenständlich die Verarbeitung von personenbezogenen Daten (Nutzeraktivitäten) durch Meta nicht nur innerhalb, sondern auch ausserhalb von «Facebook» zur Erstellung detaillierter Profile seiner Nutzer. Letzteres ist gemäss EuGH nur mit gesonderter Einwilligung zulässig.

Der EuGH hielt zum Begriff der Einwilligung gemäss Art. 4 Nr. 11 DSGVO fest, dass sie für den bestimmten Fall freiwillig, informiert und unmissverständlich sein muss. Eine beherrschende Marktstellung kann die Wahlfreiheit der Nutzer und damit die Freiwilligkeit der Einwilligung beeinträchtigen. In solchen Fällen muss der Betreiber sicherstellen, dass die Einwilligung tatsächlich freiwillig erteilt wurde, und er trägt die Beweislast dafür. Zudem müssen Nutzer die Möglichkeit haben, ihre Zustimmung zu bestimmten Datenverarbeitungen einzeln zu verweigern, ohne den Dienst vollständig aufgeben zu müssen. Entsprechend muss ihnen, allenfalls gegen ein angemessenes Entgelt, eine gleichwertige Alternative angeboten werden, die ohne solche Verarbeitungen auskommt.

Kann keine rechtsgültige Einwilligung eingeholt werden, so kann eine Verarbeitung dennoch rechtmässig sein, wenn sie erforderlich ist unter anderem für die Vertragserfüllung, zur Erfüllung einer rechtlichen Verpflichtung oder zur Wahrung berechtigter Interessen. Die Erforderlichkeit ist dabei jedoch eng auszulegen. So kann eine Datenverarbeitung durch einen Netzwerkbetreiber etwa nur dann mit der Vertragserfüllung (Nutzungsvertrag) gemäss Art. 6 Abs. 1 Bst. b DSGVO gerechtfertigt werden, wenn sie «objektiv unerlässlich ist, um einen Zweck zu verwirklichen, der notweniger Bestandteil der für diese Nutzer bestimmten Vertragsleistung ist, so dass der Hauptgegenstand des Vertrags ohne diese Verarbeitung nicht erfüllt werden könnte». Eine rechtliche Verpflichtung gemäss Art. 6 Abs. 1 Bst. c DSGVO kann eine Datenverarbeitung rechtfertigen, wenn sie zu deren Erfüllung tatsächlich erforderlich ist, die Rechtsgrundlage ein im öffentlichen Interesse liegendes Ziel verfolgt sowie in einem angemessenen Verhältnis zu diesem steht und die Verarbeitung nicht das dafür absolut Notwendige übersteigt.

Zum berechtigten Interesse gemäss Art. 6 Abs. 1 Bst. f DSGVO führte der EuGH aus, dass eine Verarbeitung nur dann als dafür erforderlich angesehen werden kann, wenn der Verantwortliche ein solches Interesse darlegt, die Verarbeitung nur in dem Mass erfolgt, wie es zur Verwirklichung dieses Interesses absolut notwendig ist, und wenn sichergestellt ist, dass die Interessen und Grundrechte der betroffenen Personen nicht überwiegen. Bei der entsprechenden Abwägung sind auch die Erwartungen der betroffenen Personen, der Umfang der Verarbeitung sowie der Schutz von Kindern und die Auswirkungen auf deren Privatleben zu berücksichtigen. In Bezug auf die Datenverarbeitung für personalisierte Werbung (zur Finanzierung der Dienstleistung) oder Netzwerksicherheit überwiegen jedoch gemäss EuGH die Interessen und Rechte der Nutzer gegenüber dem Interesse des Netzwerkbetreibers.

Ausserdem hielt der EuGH fest, dass die Verarbeitung personenbezogener Daten durch einen Betreiber eines sozialen Netzwerks als Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO betrachtet wird, wenn ein Nutzer Websites oder Apps aufruft, die sensible Daten wie ethnische Herkunft oder politische

Meinungen betreffen, und dort Daten eingibt oder Online-Bestellungen vornimmt. Eine solche Verarbeitung ist verboten, es sei denn, es gelten die Ausnahmen in Art. 9 Abs. 2 DSGVO.

Zur Frage danach, ob Daten, die ein Nutzer durch die Nutzung von Websites oder Apps (z.B. durch Betätigen von «Gefällt mir»- oder «Teilen»-Schaltflächen, welche seine Identifizierung erlauben) eingibt, als «offensichtlich öffentlich gemacht» im Sinne von Art. 9 Abs. 2 Buchst. e DSGVO gelten, stellt der EuGH fest, dass dies nur dann der Fall ist, wenn der Nutzer ausdrücklich und in Kenntnis der Sachlage entscheidet, die Daten einer unbegrenzten Zahl von Personen zugänglich zu machen. Wird keine solche Entscheidung getroffen bzw. Einwilligung erteilt, oder auch entsprechende Websites oder Apps nur aufgerufen (ohne weitergehende Interaktion), gelten die Daten nicht als öffentlich gemacht und können somit nicht rechtmässig gestützt auf Abs. 2 Bst. e verarbeitet werden.

Eine nationale Wettbewerbsbehörde kann im Rahmen der Prüfung, ob eine beherrschende Stellung missbraucht wird, auch einen Verstoss gegen die DSGVO feststellen. Sie muss dabei im Sinne einer loyalen Zusammenarbeit jedoch eine etwaige Entscheidung oder Untersuchung seitens der nach der DSGVO zuständigen Aufsichtsbehörde berücksichtigen. Diese zulässige Verknüpfung von Wettbewerbsrecht und Datenschutzrecht wurde mit Urteil des EuGH vom 4. Oktober 2024, Nr. C-21/23 (ND v. DR) bestätigt.

Quelle: Zusammenfassung des EuGH-Urteils Nr. C-252/21

f. Urteil des EuGH vom 22. Juni 2023, Nr. C-579/21 (Pankki S) – Umfang Auskunftsrecht

Das Auskunftsrecht nach DSGVO ist auch auf Datenverarbeitungen von früher anwendbar. Im Normalfall umfasst es jedoch keine Auskunft zu konkreten Mitarbeitenden eines Verantwortlichen, welche die fraglichen Daten verarbeitet haben.

Der EuGH stellt zunächst fest, dass die DSGVO auf ein Auskunftsersuchen nach Art. 15 DSGVO anwendbar ist, auch wenn die dieses Ersuchen betreffenden Verarbeitungsvorgänge schon vor dem Anwendungsdatum der DSGVO ausgeführt wurden.

Sodann stellt der EuGH fest, dass Art. 15 Abs. 1 DSGVO dahin auszulegen ist, dass Informationen, die Abfragen personenbezogener Daten einer Person betreffen und die sich auf den Zeitpunkt und die Zwecke dieser Vorgänge beziehen, Informationen darstellen, die die genannte Person nach dieser Bestimmung von dem Verantwortlichen verlangen darf. Dagegen sieht diese Bestimmung kein solches Recht in Bezug auf Informationen über die Identität der konkreten Arbeitnehmer dieses Verantwortlichen vor, die diese Vorgänge unter seiner Aufsicht und im Einklang mit seinen Weisungen ausgeführt haben, ausser wenn diese Informationen unerlässlich sind, um der betroffenen Person es zu ermöglichen, die ihr durch diese Verordnung verliehenen Rechte wirksam wahrzunehmen, und vorausgesetzt, dass die Rechte und Freiheiten dieser Arbeitnehmer berücksichtigt werden.

g. Urteil des EuGH vom 26. Oktober 2023, Nr. C-307/22 (FT) – Kopie der Patientenakte

(Vollständige) Erstkopie der Patientenakte ist kostenlos und begründungsfrei zu erstellen.

Ein Patient verlangt von seiner Zahnärztin eine unentgeltliche Kopie seiner Patientenakte, um gegen sie Haftungsansprüche wegen Fehlern geltend zu machen, die ihr bei seiner zahnärztlichen Behandlung unterlaufen sein sollen.

In seinem Urteil hat der EuGH entschieden, dass die erste Auskunft aus der Patientenakte nach Art. 12 Abs. 5 DSGVO sowie Art. 15 Abs. 1 und 3 DSGVO kostenlos zu sein hat und dass dies auch gelte, wenn der betreffende Antrag mit einem anderen als den in Satz 1 des 63. Erwägungsgrundes der DSGVO genannten Zwecken begründet wird. Der Patient ist nicht verpflichtet, seinen Antrag zu begründen. Selbst mit Blick auf den Schutz der wirtschaftlichen Interessen der Behandelnden dürfen die nationalen Regelungen dem Patienten nicht die Kosten einer ersten Kopie seiner Patientenakte auferlegen.

Des Weiteren hat der Patient das Recht, eine vollständige Kopie der Dokumente zu erhalten, die sich in seiner Patientenakte befinden, wenn dies zum Verständnis der in diesen Dokumenten enthaltenen personenbezogenen Daten erforderlich ist. Dies schliesst Daten aus der Patientenakte ein, die Informationen wie beispielsweise Diagnosen, Untersuchungsergebnisse, Befunde der behandelnden Ärzte und Angaben zu Behandlungen oder Eingriffen enthalten.

h. Urteil des EuGH vom 5. Dezember 2023, Nr. C-683/21 (Nacionalinis visuomenės sveikatos centras) und Nr. C-807/21 (Deutsche Wohnen) – Geldbussen; Haftung juristischer Personen; gemeinsame Verantwortlichkeit

Geldbussen nach DSGVO dürfen nur bei schuldhaftem Verstoss (vorsätzlich oder fahrlässig) verhängt werden. Die Haftung verantwortlicher juristischer Personen gilt für Verstösse aller ihr zurechenbaren Personen, wobei ein Verstoss nicht einer konkreten natürlichen Person zugerechnet werden muss. Zur Bestimmung einer gemeinsamen Verantwortlichkeit genügt deren faktisches Vorhandensein.

Auf die Vorlageanträge eines deutschen und eines litauischen Gerichtes hat der EuGH entschieden, dass gegen einen für die Datenverarbeitung Verantwortlichen nur dann eine Geldbusse wegen Verstosses gegen die DSGVO verhängt werden kann, wenn der Verstoss schuldhaft – also vorsätzlich oder fahrlässig – begangen wurde.

Handelt es sich bei dem Verantwortlichen um eine juristische Person, haftet diese nicht nur für Verstösse ihrer Vertreter, Leitungspersonen oder Geschäftsführer, sondern auch für Verstösse, die von jeder sonstigen Person begangen werden, die im Rahmen ihrer unternehmerischen Tätigkeit in ihrem Namen handelt. Dass der Verstoss einer identifizierten natürlichen Person zugerechnet werden kann, ist dafür jedoch keine Voraussetzung. Ausserdem kann gegen einen Verantwortlichen eine Geldbusse auch für Verarbeitungsvorgänge verhängt werden, die von einem Auftragsverarbeiter durchgeführt wurden, sofern diese Vorgänge dem Verantwortlichen zugerechnet werden können.

Zur gemeinsamen Verantwortlichkeit von zwei oder mehr Einrichtungen führt der EuGH aus, dass diese sich allein daraus ergibt, dass die Einrichtungen an der Entscheidung über die Zwecke und Mittel der Verarbeitung faktisch mitgewirkt haben. Die Einstufung als «gemeinsam Verantwortliche» setzt keine förmliche Vereinbarung zwischen den betreffenden Einrichtungen voraus.

Schliesslich muss sich die Aufsichtsbehörde bei der Bemessung der Geldbusse auf den wettbewerbsrechtlichen Begriff «Unternehmen» stützen, wenn der Adressat ein Unternehmen ist oder zu einem Unternehmen gehört. Der Höchstbetrag der Geldbusse ist auf der Grundlage eines Prozentsatzes des gesamten Jahresumsatzes zu berechnen, den das betreffende Unternehmen als Ganzes im vorangegangenen Geschäftsjahr weltweit erzielt hat.

i. EuGH-Urteil vom 14. März 2024, Nr. C-46/23 (Budapest Főváros v. Nemzeti) – Befugnisse der Aufsichtsbehörde

Zur wirksamen Durchsetzung der DSGVO darf eine Datenschutz-Aufsichtsbehörde auch von Amtes wegen Untersuchungen starten und Sanktionen erlassen.

Gemäss EuGH ist Art. 58 Abs. 2 Bst. d und g DSGVO dahingehend auszulegen, dass die Datenschutz-Aufsichtsbehörde eines Mitgliedstaats den Verantwortlichen oder Auftragsverarbeiter in Ausübung ihrer in diesen Bestimmungen vorgesehenen Abhilfebefugnisse selbst dann zur Löschung unrechtmässig verarbeiteter personenbezogener Daten anweisen darf, wenn die betroffene Person – etwa in Unkenntnis der tatsächlich verarbeiteten Daten – keinen entsprechenden Antrag auf Ausübung ihrer Rechte nach Art. 17 Abs. 1 DSGVO gestellt hat. Eine solche Löschanordnung kann sich dabei sowohl auf bei der betroffenen Person erhobene als auch auf aus einer anderen Quelle stammende Daten beziehen.

Der EuGH hält fest, dass es für Datenschutz-Aufsichtsbehörden zur Erfüllung ihrer Aufgabe, die Anwendung der DSGVO zu überwachen und durchzusetzen, erforderlich ist, dass sie über geeignete und wirksame Befugnisse verfügen, um gegen Verstösse effektiv vorgehen zu können. Diese umfassen deshalb auch Untersuchungen und Sanktionen von Amtes wegen, ohne dass ein Betroffener dies zuvor mit einer Beschwerde beantragt hätte.

j. Urteil des EuGH vom 11. Juli 2024, Nr. C-757/22 (Meta v. Verbraucherzentrale) – Datenschutzhinweise; Verbandsklagebefugnis

Zu spät, falsch oder gar nicht vorhandene Datenschutzhinweise sorgen für eine rechtswidrige Datenverarbeitung, gegen die auch eine Verbandsklage grundsätzlich zulässig ist.

Die Verbandsklagebefugnis bei DSGVO-Verstössen wurde vom EuGH bereits in der Vergangenheit bejaht. Mit diesem Urteil sorgt er nun für weitere Klarheit bezüglich der Befugnisse und Voraussetzungen für Verbandsklagen sowie der Informationspflichten der Verantwortlichen bei der Datenverarbeitung.

Der blosse Verstoss gegen die Informationspflichten, die sich aus Art. 13 und 14 DSGVO ergeben, stellt eine rechtsverletzende Datenverarbeitung dar. Das bedeutet, dass eine Daten-

verarbeitung dann rechtswidrig ist, wenn nicht spätestens zum Zeitpunkt der ersten Datenverarbeitung die Informationspflichten erfüllt werden. Zu spät, falsch oder gar nicht vorhandene Datenschutzhinweise sorgen also für eine rechtswidrige Datenverarbeitung.

Das Recht einer durch eine Verarbeitung personenbezogener Daten betroffenen Person aus Art. 12 Abs. 1 Satz 1 und Art. 13 Abs. 1 Buchst. c und e DSGVO, vom Verantwortlichen Informationen über den Zweck der Datenverarbeitung und die Empfänger personenbezogener Daten spätestens bei der Erhebung dieser Daten in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache übermittelt zu bekommen, stellt folglich ein Recht dar, bei dessen Verletzung von dem in Art. 80 Abs. 2 DSGVO vorgesehenen Verbandsklagemechanismus Gebrauch gemacht werden kann.

k. EuGH-Urteil vom 26. September 2024, Nr. C-768/21 (TR v. Land Hessen) – Entscheidungsspielraum der Aufsichtsbehörde

Es besteht kein Anspruch auf eine (bestimmte) Sanktion durch die Datenschutz-Aufsichtsbehörde gegen den Verantwortlichen.

Die Datenschutz-Aufsichtsbehörde ist gemäss EuGH nicht verpflichtet, in jedem Fall eines Verstosses gegen die DSGVO eine Abhilfemassnahme gemäss Art. 58 Abs. 2 DSGVO zu ergreifen und insbesondere eine Geldbusse zu verhängen.

So sind Art. 57 Abs. 1 Bst. a und f, Art. 58 Abs. 2 sowie Art. 77 Abs. 1 DSGVO nicht dahingehend auszulegen, dass die Aufsichtsbehörde im Fall der Feststellung einer Verletzung des Schutzes personenbezogener Daten verpflichtet ist, nach Art. 58 Abs. 2 eine Abhilfemassnahme zu ergreifen, insbesondere eine Geldbusse zu verhängen, wenn ein solches Einschreiten nicht geeignet, erforderlich oder verhältnismässig ist, um der festgestellten Unzulänglichkeit abzuhelfen und die umfassende Einhaltung dieser Verordnung zu gewährleisten.

Der Betroffene einer Datenschutzverletzung hat folglich nicht ohne weiteres Anspruch auf eine bestimmte Handlung der Aufsichtsbehörde.

l. Urteil des EuGH vom 12. September 2024, Nr. C-17/22 (HTB v. Müller) und C-18/22 (Ökorenta v. WealthCap) – Enge Auslegung des berechtigten Interesses – absolute Notwendigkeit; Rechtsprechung als rechtliche Verpflichtung

Die Berufung auf das berechtigte Interesse gemäss Art. 6 Abs. 1 Bst. f DSGVO setzt eine absolute Notwendigkeit der Datenverarbeitung und eine Interessenabwägung voraus. Bestimmte Rechtsprechung kann eine rechtliche Verpflichtung gemäss Art. 6 Abs. 1 Bst. c DSGVO darstellen.

Eine Verarbeitung kann nur dann auf ein berechtigtes Interesse gestützt werden, wenn sie zur Verwirklichung des berechtigten Interesses absolut notwendig ist und unter Würdigung aller relevanten Umstände die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person(en) gegenüber diesem berechtigten Interesse nicht überwiegen. Das

Gericht stellte im vorliegenden Fall fest, dass es dem Gesellschafter eines Investmentfonds, der Informationen über einen anderen, an diesem Fonds über eine Treuhandgesellschaft mittelbar beteiligten Anteilseigner erhalten möchte, insbesondere möglich wäre, diesen Fonds oder diese Gesellschaft unmittelbar aufzufordern, seine Anfrage an den betreffenden Gesellschafter weiterzuleiten, um ihn kennenzulernen oder sich mit ihm auszutauschen. Dieser könnte dann frei entscheiden, ob er mit dem anfragenden Gesellschafter Kontakt aufnehmen möchte oder nicht. Die automatische Weitergabe der Kontaktdaten war somit zur Verwirklichung des berechtigten Interesses nicht absolut notwendig.

Des Weiteren hielt der EuGH fest, dass eine rechtliche Verpflichtung als Rechtsgrundlage für eine bestimmte Datenverarbeitung auch in Betracht komme, wenn sie sich aus der Rechtsprechung eines Mitgliedstaats ergebe, sofern diese Rechtsprechung klar und präzise sei, ihre Anwendung für die Rechtsunterworfenen vorhersehbar sei und sie ein im öffentlichen Interesse liegendes Ziel verfolge, zu dem sie in einem angemessenen Verhältnis steht.

m. Urteil des EuGH vom 4. Oktober 2024, Nr. C-621/22 (Koninklijke v. niederländische Datenschutzbehörde) – Enge Auslegung des berechtigten Interesses – kein milderes Mittel

Art. 6 Abs. 1 Bst. f DSGVO setzt voraus, dass das berechtigte Interesse nicht mit einem milderen Mittel als der geplanten Datenverarbeitung erreicht werden kann.

Der EuGH weist unter Bezugnahme auf seine Entscheidung in der Rechtssache C-252/21 (Meta Platforms u.a.) darauf hin, dass die Rechtsgrundlagen aus Art. 6 Abs. 1 Bst. b bis f DSGVO eng auszulegen sind. Die Erforderlichkeit einer bestimmten Datenverarbeitung des Verantwortlichen ist jeweils nur dann zu bejahen, wenn keine zumutbaren Mittel vorliegen, die ebenso geeignet sind und weniger stark in die Grundrechte und Grundfreiheiten der betroffenen Personen eingreifen. Auch ein rechtskonformes, wirtschaftliches Interesse kann ein berechtigtes Interesse des Verantwortlichen darstellen.

Das Gericht stellte im vorliegenden Fall fest, dass es einem Sportverband möglich gewesen wäre, seine Mitglieder bereits im Voraus zu informieren und zu fragen, ob ihre Daten für Werbe- oder Marketingzwecke an Dritte weitergegeben werden dürfen. Als verantwortliche Stelle ist deshalb stets zu prüfen, ob die berechtigten Interessen gegebenenfalls durch ein milderes, weniger eingriffsintensives Mittel erreicht werden können.

n. Urteil des EuGH vom 4. Oktober 2024, Nr. C-21/23 (ND v. DR) – Gesundheitsdaten bei Online-Arzneimittelbestellungen; DSGVO und Wettbewerbsrecht

Sämtliche eingegebenen Bestelldaten werden bei einer Online-Arzneimittelbestellung zu Gesundheitsdaten gemäss Art. 9 Abs. 1 DSGVO. Die DSGVO steht der wettbewerbsrechtlichen Verfolgung von Datenschutzverstössen nicht entgegen.

Mit diesem Urteil verschärft der EuGH die datenschutzrechtlichen Anforderungen an den Online-Handel. Online-Apotheken müssen den Gesundheitsdatenschutz einhalten, auch bei

Präparaten, die nur apotheken- und nicht rezeptpflichtig sind. Anlass für dieses Urteil war der Vertrieb von apothekenpflichtigen Arzneimitteln durch eine Apotheke über Amazon. Ein Mitbewerber erhob eine Unterlassungsklage gegen die vertreibende Apotheke, solange nicht sichergestellt sei, dass die Kunden vorab die Möglichkeit hätten, in die Verarbeitung von Gesundheitsdaten einzuwilligen. Die unzulässige Verarbeitung von Gesundheitsdaten sei unlautererer Wettbewerb.

Der EuGH gelangte zur Ansicht, dass bei einer Bestellung von apothekenpflichtigen Arzneimitteln über eine Online-Plattform die dazu angegebenen Kundendaten (wie z.B. Name, Lieferadresse und für die Individualisierung der Arzneimittel notwendige Informationen) Gesundheitsdaten darstellen. Durch die Verarbeitung dieser Daten können Informationen über den Gesundheitszustand einer natürlichen Person offengelegt werden, und zwar unabhängig davon, ob diese Informationen den Käufer betreffen oder eine andere Person, für die diese Bestellung getätigt wird. Da die Verarbeitung von Gesundheitsdaten ein hohes Schutzniveau verlangt, erfordert sie eine ausdrückliche, darauf ausgerichtete Einwilligung. Der EuGH folgte damit seiner strengen Linie der weiten Auslegung des Begriffs der Gesundheitsdaten und lässt hier auch unsichere, hypothetische Rückschlussmöglichkeiten auf Krankheiten genügen – unabhängig davon, ob der jeweilige Verantwortliche gesundheitsspezifische Schlüsse aus den Bestelldaten ziehen will oder nicht.

In Bezug auf das Wettbewerbsrecht beschied das Gericht, dass die Mitgliedstaaten den Mitbewerbern eines mutmasslichen Verletzers der DSGVO die Möglichkeit einräumen können, diesen Verstoss als verbotene unlautere Geschäftspraxis gerichtlich zu beanstanden. Nach Ansicht des EuGH trägt die Unterlassungsklage eines Mitbewerbers zur Einhaltung der materiellen Bestimmungen der DSGVO und damit dazu bei, die Rechte der betroffenen Personen zu stärken und ihnen ein hohes Schutzniveau zu gewährleisten, auch wenn die Unterlassungsklage dem Ansinnen nach lediglich einen lauteren Wettbewerb sicherstellen wollte. Die DSGVO steht somit der wettbewerbsrechtlichen Verfolgung von Datenschutzverstössen nicht entgegen und andere Pharmazeuten können daher gegen Verstösse von Konkurrenten klagen.

o. Urteil des EuGH vom 4. Oktober 2024, Nr. C-446/21 (Schrems v. Meta) – Grundsätze der Datenverarbeitung; Verwendung von durch die betroffene Person selbst veröffentlichten personenbezogenen Daten

Selbst bei einer grundsätzlichen Einwilligung in die Verarbeitung von personenbezogenen Daten darf keine grenzenlose Verarbeitung zum Zweck der personalisierten Werbung vorgenommen werden. Auch eine offensichtlich öffentlich gemachte Äusserung (Art. 9 Abs. 2 Bst. e DSGVO) führt nicht zu einer Einwilligung im Sinne von Art. 9 Abs. 2 Bst. a DSGVO.

Der EuGH kam zum Schluss, dass selbst bei anderweitig rechtmässiger Verarbeitung von personenbezogenen Daten, die der Betreiber einer Onlineplattform von einer betroffenen Person oder von Dritten erhält, diese Verarbeitung hinsichtlich der Datenmenge und zeitlichen Dauer nicht unbeschränkt sein darf, sondern ihre Grenzen in den Grundsätzen von Art. 5 DSGVO zu Zweckbezogenheit, Datenminimierung und Speicherbegrenzung findet. So verhindern diese Grundsätze einerseits eine mengenmässig unbegrenzte Datenerfassung einschliesslich besonderer Kategorien personenbezogener Daten, wenn diese zur

Zweckerreichung gar nicht erforderlich sind, und andererseits auch eine zeitlich unbefristete Datenspeicherung, welche zur Zweckerreichung nicht erforderlich ist. Beides würde einen unverhältnismässigen Eingriff in die Rechte und Freiheiten einer betroffenen Person darstellen. Was genau aber eine angemessene Speicherfrist für einen bestimmten Zweck ist (vorliegend die Schaltung personalisierter Werbung), muss jeweils im Einzelfall und gegebenenfalls von den nationalen Gerichten geklärt werden.

Betreffend die öffentliche Äusserung des Beschwerdeführers zu seiner sexuellen Orientierung im Rahmen einer Podiumsdiskussion ist der EuGH der Ansicht, dass die offensichtliche Öffentlichkeit der Äusserung gemäss Art. 9 Abs. 2 Bst. e DSGVO grundsätzlich zur Rechtmässigkeit der Verarbeitung dieser Daten führt. Da es sich bei dieser Bestimmung jedoch um eine Ausnahme von einem Verbot handelt, ist sie eng auszulegen. So berechtigt eine offensichtlich öffentlich gemachte Äusserung den Betreiber einer Online-Plattform nicht dazu, auch andere personenbezogene Daten zu verarbeiten, die sich auf die sexuelle Orientierung dieser Person beziehen (und die er allenfalls mithilfe von Cookies, Pixel oder Social Plug-ins von Anwendungen und Websites Dritter erhalten hat), um gestützt darauf personalisierte Werbung zu schalten. Der EuGH stellte zudem klar, dass eine offensichtlich öffentlich gemachte Äusserung nicht zu einer ausdrücklichen Einwilligung im Sinne von Art. 9 Abs. 2 Bst. a DSGVO führt. Ausserdem hielt er erneut fest, dass das grundsätzliche Verbot der Verarbeitung besonderer Kategorien personenbezogener Daten aus Art. 9 Abs. 1 DSGVO unabhängig davon gilt, ob die Information richtig ist oder nicht und ob der Verantwortliche überhaupt die Absicht hatte, solche Datenkategorien zu erheben.

p. Urteil des EuGH vom 4. Oktober 2024, Nr. C-507/23 (A v. Patērētāju) – Recht auf Schadenersatz

Definition Schaden; Entschuldigung als Ersatz eines immateriellen Schadens; Bemessung.

Gemäss EuGH reicht ein Verstoss gegen Bestimmungen der DSGVO für sich genommen nicht aus, um einen „Schaden“ im Sinne von Art. 82 Abs. 1 DSGVO darzustellen.

Ist jedoch ein Schaden eingetreten, so kann auch eine Entschuldigung einen angemessenen Ersatz für einen immateriellen Schaden darstellen, insbesondere, wenn es nicht möglich ist, die Lage von vor dem Eintritt des Schadens wiederherzustellen. Dies bedingt jedoch, dass diese Form des Schadenersatzes geeignet ist, den der betroffenen Person entstandenen Schaden in vollem Umfang auszugleichen.

Die Haltung und Beweggründe des Verantwortlichen dürfen jedoch bei der Bemessung des Schadenersatzes keine Berücksichtigung finden. Insbesondere darf der betroffenen Person deswegen kein geringerer Schadenersatz gewährt werden als der Schaden, der ihr konkret entstanden ist.

q. Urteil des EuGH vom 28. November 2024, Nr. C-169/23 (Nemzeti v. UC) – Ausnahme von der Informationspflicht bei nicht bei der betroffenen Person erhobenen Daten

Die Ausnahme von der Informationspflicht des Verantwortlichen gemäss Art. 14 Abs. 5 Bst. c DSGVO umfasst auch vom Verantwortlichen selbst erzeugte Daten. Wird diese Ausnahme in Anspruch genommen, können die Datenschutzbehörden überprüfen, ob das nationale Recht geeignete Massnahmen zum Schutz der berechtigten Interessen der betroffenen Person vorsieht.

Laut EuGH ist Art. 14 Abs. 5 Bst. c DSGVO dahingehend auszulegen, dass sich diese Ausnahme von der Informationspflicht des Verantwortlichen gegenüber der betroffenen Person auf alle personenbezogenen Daten erstreckt, die der Verantwortliche nicht direkt bei der betroffenen Person erhoben hat, unabhängig davon, ob die Daten bei einer anderen Person als der betroffenen Person erhoben wurden oder ob sie vom Verantwortlichen selbst im Rahmen der Erfüllung seiner Aufgaben erzeugt wurden.

Der EuGH stellte zudem fest, dass die Datenschutzbehörden das Recht haben zu prüfen, ob die Anforderungen von Art. 14 Abs. 5 Bst. c DSGVO erfüllt sind, insbesondere ob das Recht des jeweiligen Mitgliedstaats geeignete Massnahmen zum Schutz der berechtigten Interessen der betroffenen Person vorsieht.