DATENSCHUTZSTELLE
FÜRSTENTUM LIECHTENSTEIN

Judikaturspiegel zum europäischen Datenschutzrecht

Ausgewählte Entscheidungen Europäischer Gerichte und Höchstgerichte

(2018 – 2020)

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 (aus dem Zeitraum 2018 bis 2020) in Kurzfassung vorzustellen bzw. wesentliche Passagen der Entscheidungen hervorzuheben. Es besteht dabei kein Anspruch auf Vollständigkeit. Die angeführten Entscheidungen nationaler Gerichte und Höchstgerichte 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 vorbehaltlos für inländische Rechtssachen übernehmen lassen.

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 Judikaturbesprechung oder Glossierung zur Hand geben soll.

Sie finden nachstehend Entscheidungen von Gerichten und Höchstgerichten aus Deutschland, Österreich und Frankreich. Nur punktuell berücksichtigt wurde die rezente Judikatur des EFTA-Gerichtshofs; unberücksichtigt blieb die Rechtsprechung des EuGH sowie des EGMR. Eine Zusammenfassung der EGMR-Rechtsprechung zu Art. 8 EMRK (Recht auf Wahrung des Privat- und Familienlebens) finden Sie über: https://www.echr.coe.int/documents/fs_data_eng.pdf (Stand Mai 2020).

Zur leichteren Handhabung wurden die jeweiligen Fundstellen (Stichtag 10. Dezember 2020) via Hyperlink in den Untertiteln eingearbeitet. Dies ermöglicht den interessierten Leserinnen und Lesern, leichter weitergehende Informationen zur betreffenden Entscheidung oder der angeführten Pressemitteilung zu erlangen.

Eine Haftung für fehlerhafte Übersetzungen fremdsprachiger Judikatur und rechtsirrige Darstellung ausländischer Bestimmungen kann von der Datenschutzstelle nicht übernommen werden.

Inhaltsübersicht

I. Liechtenstein

Für Liechtenstein liegt bislang keine Rechtsprechung des StGH zur DSGVO vor. Die Entscheidung des StGH vom 3. Dezember 2019, StGH 2019/057 befasste sich noch mit der alten Rechtslage und sieht lediglich einen punktuellen Verweis auf das Inkrafttreten der DSGVO vor).

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-GH 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 gem. Art. 78 Abs. 1 DSGVO wird, keinerlei Kosten im Zusammenhang mit diesem Verfahren auferlegt werden (Spruchpunkt 2).

II. Deutschland

A. Bundesverfassungsgericht

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 veröffentlichtem) Beschluss hat die 2. Kammer des Ersten Senats einen Antrag auf vorläufige Ausserkraftsetzung des Vollzugs neu in das SGB V eingefügter 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 Verfahren 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 Tele-**

kommunikationsüberwachung 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 hinrei-

chend 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. Bundesgerichtshof

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

Einwilligungserfordernis 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.

Auf die Frage, ob es sich bei den Informationen um personenbezogene Daten handelt, kommt es nach der Entscheidung des Gerichtshofs in diesem Zusammenhang nicht an. Der richtlinienkonformen Auslegung des § 15 Abs. 3 Satz 1 TMG steht nicht entgegen, dass der deutsche Gesetzgeber bisher keinen Umsetzungsakt vorgenommen hat. Denn es ist anzunehmen, dass der Gesetzgeber die bestehende Rechtslage in Deutschland für richtlinienkonform erachtete. Mit dem Wortlaut des § 15 Abs. 3 Satz 1 TMG ist eine entsprechende richtlinienkonforme Auslegung noch vereinbar. Im Fehlen einer (wirksamen) Einwilligung kann im Blick darauf, dass der Gesetzgeber mit § 15 Abs. 3 Satz 1 TMG das unionsrechtliche Einwilligungserfordernis umgesetzt sah, der nach dieser Vorschrift der Zulässigkeit der Erstellung von Nutzungsprofilen entgegenstehende Widerspruch gesehen werden.

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

Achtung: Die für das deutsche Verfahren einschlägige RL 2009/136/EG wurde bisher *(Stand: Dezember 2020)* nicht ins EWR-Abkommen übernommen; es fehlt daher in Liechtenstein an einer nationalen Umsetzung (bspw. im KomG oder anderen einschlägigen Gesetzen).

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 Bundesgerichtshofs 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. Bundessozialgericht

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

D. 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 Steuerfahndung

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 Begeh-**

ren 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 gem. § 208 Abs. 1 Satz 1 Nr. 1 AO eingeleitet (und noch nicht abgeschlossen) wurde, wird die Steuerfahndung auch in diesem Verfahren tätig, selbst wenn sie in diesem Zusammenhang Besteuerungsgrundlagen ermittelt (Rz 16, mit weiteren Nachweisen).

E. Bundesarbeitsgericht

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 Ausschusses 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).

Desweiteren 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. Verwaltungsgerichtshof

Beschluss des VwGH vom 24. April 2020, Ra 2017/04/0143 – Patientendokumentation, Auskunftsrecht

Datenübermittlung in Unternehmenssphäre ist auskunftspflichtig

Das Auskunftsbegehren einer Patientin betreffend die Übermittlung von Zugriffslisten auf das im Krankenhaus verwendete Patientendokumentationssystem blieb teilweise unbeantwortet, weshalb sie Beschwerde (nach alter österreichischer Rechtslage) erhob.

«*Zur begehrten Beauskunftung interner Zugriffe verwies das Bundesverwaltungsgericht darauf, dass Abfragen durch Mitarbeiter des Auftraggebers, die sich innerhalb des ursprünglichen Aufgabengebietes bewegen, nicht der Auskunftspflicht gemäss § 26 DSG 2000 unterlägen, solange sie keine Übermittlungen im Sinn des § 4 Z 12 DSG 2000 darstellten.*» (Rz 12)

Der VwGH verwies in der rechtlichen Würdigung auf seine bestehende Judikatur (VwGH 28.4.2009, 2005/06/0194) zum Auskunftsrecht nach § 26 Abs. 1 DSG 2000, wonach dieses «*als Recht auf Anführung ‚allfällige(r) Empfänger oder Empfängerkreise von Übermittlungen' festgelegt ist, und in § 4 Z. 12 DSG 2000 das ‚Übermitteln von Daten' als ‚die Weitergabe von Daten einer Datenanwendung an andere Empfänger als den Betroffenen, den Auftraggeber oder einen Dienstleister, insbesondere auch das Veröffentlichen solcher Daten*».

Dies näher ausführend, liegt «*ein ‚Übermitteln von Daten' auch dann vor, wenn Daten innerhalb der Sphäre ein und desselben Auftraggebers für ein anderes Aufgabengebiet des Auftraggebers verwendet werden*.»

B. Bundesverwaltungsgericht

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 herangezogenen **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 02. 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 gem. 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. Teilerkenntnis des BVwG vom 26. November 2020, W258 2217446-1/35E – keine Rechtsgrundlage zur Verarbeitung von Daten betreffend «*Parteiaffinität*»

«Parteiaffinität» als besondere Kategorie personenbezogener Daten gem. Art. 9 DSGVO

Das BVwG bestätigte (teilweise) einen Bescheid der Datenschutzbehörde, wonach Daten zur «*Parteiaffinität*» besondere Kategorien personenbezogener Daten i.S.v. Art. 9 DSGVO darstellen. Als solche unterliegen sie dem darin normierten Verarbeitungsverbot und wurden von der verantwortlichen Österreichischen Post AG unrechtmässig verarbeitet. Der Unionsgesetzgeber beabsichtigte bei Umsetzung der DSGVO durch die Verwendung des Ausdrucks «*alle Informationen*», «*dem Begriff der personenbezogenen Daten eine weite Bedeutung beizumessen*». Aus der „*Parteiaffinität*“ könne mit hinreichender Wahrscheinlichkeit die politische Meinung abgeleitet werden, «*weshalb besondere Kategorien personenbezogener Daten iSd Art. 9 DSGVO vorliegen*». Die gezielte Zustellung von Werbung politischer Parteien nach der sohin ermittelten «*Parteiaffinität*» verwirkliche eine Gefahr, die durch die Umsetzung von Art. 9 DSGVO vermieden werden sollte.

Die gegenständlich herangezogenen Bestimmungen der österreichischen Gewerbeordnung (§ 151 GewO) stellen keine Rechtsgrundlage dar, welche eine Verarbeitung besonderer Kategorien personenbezogener Daten erlaubten.

Da sich fallgegenständlich die Österreichische Post AG auf keine der sonst in Frage kommenden Ausnahmebestimmungen des Art. 9 Abs. 2 DSGVO vom Verarbeitungsverbot besonderer Kategorien von Daten des Art. 9 Abs. 1 DSGVO berufen konnte, insbesondere auch keine Einwilligung für die Verarbeitung durch die Betroffenen vorlag, erwies sich die Verarbeitung der Daten zur «*Parteiaffinität*» als rechtswidrig.

Desweiteren führte das BVwG hinsichtlich der Abhilfemassnahmen gem. Art. 58 DSGVO zusammengefasst aus, dass der öDSB «*auch im Rahmen eines amtswegigen Einschreitens die Kompetenz zu*(kommt), *Rechtsverletzungen in einer der Rechtskraft fähigen Weise festzustellen*.»

Hinsichtlich der im Bescheid der öDSB angeordneten Löschverpflichtung sowie der Anordnung auf Ergänzung des Verarbeitungsverzeichnisses wird gesondert entschieden. Im Teilerkenntnis bestätigte das BVwG die von der öDSB festgestellten Rechtswidrigkeiten, ausgenommen bezüglich der Pflicht zur Durchführung einer Datenschutzfolgenabschätzung; der diesbezüglich Spruchpunkt wurde ersatzlos behoben.

Quelle: **Newsletter 2020/4 der österreichischen Datenschutzbehörde**

f. Erkenntnis des BVwG vom 26. November 2020, W258 2227269-1/14E – Nationales Verwaltungsverfahrensrecht; Aufhebung hoher Geldbusse wegen Verarbeitung von Daten zur «*Parteiaffinität*» durch die Österreichische Post AG.

Vorbemerkung: Den Ausführungen zur gegenständlichen Entscheidung ist vorauszuschicken, dass das BVwG sich vorrangig mit Fragen des nationalen österreichischen Verwaltungsverfahrensrechts auseinanderzusetzen hatte.

Erfordernis der Benennung einer natürlichen Person, deren Zuwiderhandeln einer juristischen Person zugerechnet wird.

Die österreichische Datenschutzbehörde erliess gegen die österreichische Post AG wegen der unrechtmässigen Verarbeitung besonderer Kategorien personenbezogener Daten und weiterer Datenschutzverletzungen ein (Verwaltungs-)Straferkenntnis und sprach darin eine Geldbusse in der Höhe von EUR 18 Millionen. Dieses Erkenntnis wurde vom BVwG behoben und das Verfahren eingestellt.

Die öDSB führte in ihrem Straferkenntnis etwa folgendes aus: In der Unterlassung der Verantwortlichen (d.h. diverser namentlich genannter aussenvertretungsbefugter Personen, wie der Prokuristin, diverser Personen mit Leitungsfunktion in Fachbereichen, aber auch der Datenschutzbeauftragten) eine Prüfung auf Datenschutzkonformität zu veranlassen bzw. eine eingehende und fundierte rechtliche Auseinandersetzung mit allfälligen rechtlichen Risiken vorzunehmen, verwirklicht sich «*das subjektiv vorwerfbare Verhalten*». Darin ist «*in Bezug auf den Umfang der Datenverarbeitungen, der Anzahl der Betroffenen und der für diese*

potenziell hieraus resultierenden Gefahren für deren grundrechtlich geschützten Rechtspositionen (ein*) grob fahrlässiges Verhalten*» zu erkennen (siehe 2.17).

Das BVwG begründet die Aufhebung des Straferkenntnisses damit, dass «*die natürliche Person, deren Verstoss gegen die DSGVO der* (Verantwortlichen) *zugerechnet werden soll, nicht benannt* (wurde). *Das Straferkenntnis erwies sich daher als rechtswidrig*.» (3.6.)

In Bezugnahme auf die Rechtsprechung des VwGH vom 29. März 2019, Ro 2018/02/0023 sowie vom 12. Mai 2020, Ro 2019/04/0229 (siehe oben III.A.a.) hielt das BVwG fest, dass es nicht ausreicht festzustellen, dass irgendeine Person aus einem Kreis natürlicher Personen (bspw. eine Führungsperson) die Tat begangen hat, sondern «*es muss die handelnde Person konkret bestimmt sein*». Die darüber hinaus von der öDSB festgestellte Verwaltungsübertretungen bzw. der eigentliche Tatvorwurf wurden der Sache nach vom BVwG nicht behandelt.

C. Oberster Gerichtshof

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

Keine Haushaltsausnahme im zivilgerichtlichen Verfahren; gerichtliche Geltendmachung von Löschrecht

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 sind diese Informationen als besonders sensible Daten gem. 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 gem. 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 insbesondere 7.1.)

Quelle: OGH 20.12.2018, 6 Ob 131/18k.

b. Beschluss des OGH vom 29. August 2019, 6 Ob 152/19z – Medienprivileg – keine Derogation von Urheberrecht durch DSGVO

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.*»

Quelle: OGH 29.08.2019, 6 Ob 152/19z.

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 gem. 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*».

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

Quelle: OGH 17.11.2020, 6 Ob 150/19f.

d. Urteil des OGH vom 27. November 2019, 6 Ob 217/19h – Bonitätsauskunft, Schadenersatz und Beweislastumkehr gem. Art. 82 DSGVO

Beweislastumkehr gem. Art. 82 DSGVO

Die Verarbeitung personenbezogener Daten über eine sogenannte «Wirtschaftsauskunftei», durch Bereitstellung von Daten betreffend die Kreditwürdigkeit/Bonität einer natürlichen Person hat dem allgemeinen Grundsatz von Treu und Glauben gem. Art. 5 Abs. 1 Bst. a DSGVO zu entsprechen. Die fallgegenständlich beklagte Wirtschaftsauskunftei hatte vor Verarbeitung der Dateien bzw. Auskunftserteilung jedoch keinen direkten Kontakt mit dem klagenden Betroffenen, über den eine Bonitätsauskunft (Auskunft über ein angeblich behängendes Inkassoverfahren) erteilt wurde.

«*Ohne diese negative Auskunft wäre* (der vom Kläger gewünschte) *Kreditvertrag zustande gekommen*.» Der nachfolgend geschlossene Kreditvertrag bei einer anderen Bank sei ungünstiger ausgefallen, weshalb dem Kläger Mehraufwendungen entstanden seien. Zudem wurde auf Grundlage der erkannten Datenschutzverletzung (Verarbeitung wider Treu und Glauben) Anspruch auf immateriellen Schadenersatz in der Höhe von EUR 2.000 begehrt.

Das Ersturteil erwuchs in seinem klagstattgebenden Teil (wonach die Beklagte zur Zahlung von EUR 2.000 verpflichtet wurde) mangels Anfechtung in Rechtskraft. Über Berufung des Klägers bestätigte das Berufungsgericht den klagabweisenden Teil des Urteils. Nach Verwerfung einer Beweis- und Mängelrüge erwog es in rechtlicher Sicht, dass das Vorliegen einer unzulässigen Verarbeitung noch nicht für das Entstehen einer Ersatzpflicht genüge. Weder für das Vorliegen eines Schadens noch für die Kausalität erscheine die Annahme einer Beweislastumkehr sachgerecht. Damit gingen die vom Erstgericht getroffenen Negativfeststellungen zu Lasten des Klägers.

Da zur Frage der Beweislastverteilung bei Geltendmachung eines Anspruchs gem. Art. 82 DSGVO keine höchstgerichtliche Judikatur vorlag, wurde die ordentliche Revision zugelassen.

Der OGH führte zur **Beweislastverteilung des Art. 82 DSGVO** im Wesentlichen aus, dass «(n)*ach Abs 3 dieser Bestimmung* (…) *der* ***Verantwortliche oder der Auftragsverarbeiter***

von** der **Haftung** gemäss Abs 2 der Norm **befreit (wird), ***wenn er nachweist**, dass er in **keinerlei Hinsicht** für den Umstand, durch den der Schaden eingetreten ist, **verantwortlich** ist*.» Darüber hinaus wurde mit Verweis auf 6 Ob 131/18k und 6 Ob 91/19d klargestellt, «*dass Art 82 DSGVO als Ergänzung zum nationalen Schadenersatzrecht als eine Art lex specialis eines datenschutzrechtlichen Schadenersatzrechts zu sehen ist*». Gestützt auf die im österreichischen Schrifttum vertretene herrschende Meinung sieht Art. 82 DSGVO «*nur eine Beweislastumkehr in Bezug auf das Verschulden, nicht jedoch hinsichtlich der anderen anspruchsbegründenden Voraussetzungen vor*» (4.3.). **Für die Kausalität ist keine Beweislastumkehr abzuleiten**. Die **Beweislast bezüglich der haftungsbegründenden Tatsachen trifft den Kläger**, d.h. «*der Eintritt eines (materiellen oder immateriellen) Schadens, sowie die (Mit-)Ursächlichkeit des Verhaltens des Schädigers am eingetretenen Schaden im Sinne einer adäquaten Kausalität*.» (5.2.).

Mit Verweis auf seine ältere Judikatur bestätigte der OGH zur neuen Rechtslage, dass eine Datenverarbeitung nach Treu und Glauben eine Benachrichtigung der Betroffenen erfordert. «*Die Eintragung in die Warnliste ist rechtswidrig und der Bank subjektiv vorwerfbar, wenn sie ohne* (…) *Benachrichtigung erfolgt*.» (mVa OGH 6 Ob 275/05t, 6 Ob 247/08d).

Quelle: OGH 27.11.2020, 6 Ob 217/19h.

D. Oberlandesgericht Innsbruck

Urteil des Oberlandesgerichts Innsbruck vom 13. Februar 2020, AZ: 1 R 192/19b – Schadenersatz bei Datenschutzverletzung; Daten zur «Parteiaffinität»

Ein Betroffener begehrte von der österreichischen Post AG wegen der Verarbeitung seiner personenbezogenen Daten zur Parteiaffinität gemäss Art. 83 DSGVO Schadenersatz in der Höhe von EUR 2.500. Das Landesgericht Feldkirch sprach dem Kläger in erster Instanz einen Betrag von EUR 800 zu.

Das OLG Innsbruck folgte der dagegen gerichteten Berufung der österreichischen Post AG und wies die Klage kostenpflichtig ab. Das OLG Innsbruck als Berufungsgericht schloss die Möglichkeit der Geltendmachung von Schadenersatzansprüchen gemäss Art. 83 DSGVO nicht kategorisch aus, aber der Kläger habe dazu das Eintreten des Schadens und dessen Höhe zu beweisen.

Der alleinige Umstand, dass eine Datenschutzverletzung festgestellt werden könne, reiche zur Geltendmachung von Schadenersatzansprüchen nicht aus. Ein Datenschutzverstoss müsse über ein «*Mindestmass an persönlicher Beeinträchtigung des Geschädigt*en» hinausgehen, die blosse Geltendmachung «*negativer Gefühle*» reiche dazu nicht aus. Es fehlte im Klagevorbringen an einer entsprechenden Darlegung bzw. eines Beweises eines solchen Eingriffs (RIS-Rechtssatz RI0100071).

Quelle: Newsletter 2020/2 der österreichischen Datenschutzbehörde

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/**)

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 gem. 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 – Verwendung von Drohnen zur Identifikation von Personen unzulässig

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 Ein-

willigung 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 Datenverarbeitung 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 – Generelles Verbot von Cookie-Walls durch behördliches «soft-law» unzulässig

Unzulässigkeit allgemeiner und absoluter Verbote (z.B. 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 französischen Datenschutzaufsichtsbehörde (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 französische Datenschutzbehörde (CNIL) kann auf Grundlage der DSGVO keine allgemeine Leitlinie bzw. Richtlinien erlassen, die ein Verbot von «Cookie-Walls» vorsieht. Nach Rechtsan-

sicht 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 Datenschutzbehörde (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)