„Es war einmal … und: Was seither geschah …“,
oder: Österreichisches Datenschutzrecht seit der DSGVO / DSG (2018)
und der liebe EuGH

August 2019

1. „Datenschutzgesetz-Novelle 2019“

1.1. Die DSGVO umfasst ausschließlich Daten natürlicher Personen. Das DSG schützt hingegen (schon immer) auch personenbezogene Daten von juristischen Personen. Die in der Regierungsvorlage [Link] zur „Datenschutzgesetz-Novelle 2019“ noch geplante „Einschränkung“ des Grundrechts (mit Drittwirkung) auf Datenschutz auf natürliche Personen (also ohne juristische Personen) wurde nicht Gesetz.

1.2. Mit dem Bundesgesetzblatt I 2019/14 vom 15. Jänner 2019 [Link] wurde das DSG (2018) wieder geändert. Wichtig ist die mit Aufhebung der Regelungen zum räumlichen Anwendungsbereich des österreichischen Datenschutzgesetzes zum 01.01.2020: Der § 3 DSG bringt (bis 31.12.2019) ein „rechtssichereres Mehr“ gegenüber der Datenschutz-Grundverordnung (DSGVO): Er schafft eine klare Abgrenzung der nationalen Datenschutzgesetze der EU-Mitgliedsstaaten gegenüber dem österreichischen Datenschutzgesetz, wie folgt:

- Die Bestimmungen des DSG sind auf die Verwendung von personenbezogenen Daten in Österreich anzuwenden.
- Darüber hinaus ist das DSG auf die Verwendung von Daten im Ausland anzuwenden, soweit diese Verwendung in anderen Mitgliedstaaten der Europäischen Union für Zwecke einer in Österreich gelegenen Haupt- oder Zweigniederlassung geschieht.
- Abweichend davon ist das Recht des Sitzstaates auf eine Datenverarbeitung in Österreich anzuwenden, wenn sie hier zu einem Zweck verwendet/ verarbeitet wird, der keiner in Österreich gelegenen Niederlassung zuzurechnen ist.
- Weiters ist das DSG nicht anzuwenden, wenn personenbezogene Daten durch Österreich nur durchgeführt werden.

Ab 1.1.2020 wird nicht mehr ausdrücklich geregelt sein, wie die Anwendbarkeit der nationalen Datenschutzgesetze abgegrenzt werden soll. Anders sehen es die Erläuterungen [Link] zur Aufhebung des § 3 DSG: „*Der räumliche Anwendungsbereich ergibt sich bereits unmittelbar anwendbar aus Art. 3 DSGVO.*“ Aus dieser Bestimmung ergibt sich aber gerade keine Abgrenzung des räumlichen Anwendungsbereichs zwischen den nationalen Datenschutzgesetzen der EU-Mitgliedsstaaten.

2. Österreichische Datenschutzbehörde (DSB) zur Datenschutz-Folgenabschätzung

2.1. Art 35 DSGVO normiert, dass der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchzuführen hat, wenn eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

2.2. Die DSB hat eine Datenschutz-Folgenabschätzung-Ausnahmenverordnung (DSFA-AV) [Link] erlassen, in der eine Liste der Arten von Verarbeitungsvorgängen enthalten ist, für die keine Datenschutz-Folgenabschätzung erforderlich ist (Erläuterungen zum Entwurf hier [Link]).

2.3. Weiters hat die DSB eine Verordnung über Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist (DSFA-V) [Link] erlassen. Das ist eine Liste aller Arten von Verarbeitungsvorgängen, für die jedenfalls eine Datenschutz-Folgenabschätzung erforderlich ist (Erläuterungen zum Entwurf hier [Link]). Zu kritisieren ist dabei, dass der Katalog äußerst unbestimmt und zum Teil praktisch einfach zu weitreichend ist.

3. Wichtige Spruchpraxis der österreichischen Gerichte und Behörden – mit Anmerkungen von GEISTWERT

Einleitende Anmerkung von GEISTWERT: die österreichischen Behörden und Gerichte waren und sind wohl wieder die ersten in Europa, welche über „neue Rechtsfragen“ entscheiden (so schon zum nicht-eingetragenen Geschmacksmuster, keyword-Advertising, Domain Grabbing, uvm): Hintergrund ist, dass der österreichische Gesetzgeber keine Übergangsregelungen vorgesehen hat und daher seit dem 25. Mai 2018 bei allen anhängigen Verfahren nach der neuen Rechtslage – also nach DSGVO bzw. DSG (2018) – entschieden wird:

3.1. Wohl allererste Entscheidung zur DSGVO: Datenschutzbehörde (DSB) - Verhältnis Telekommunikationsrecht zu DSGVO und Speicherdauer (DSB-D216.471/0001-DSB/2018 am 28.05.2018 [Link])

Die Datenschutzbehörde entscheidet über die Datenschutzbeschwerde der Alice A*** (Beschwerdeführerin) vom 6. Juli 2017 gegen die N***-Telecom GmbH (Beschwerdegegnerin) wegen Verletzung im Recht auf Geheimhaltung in Folge Speicherung von personenbezogenen Daten über einen gesetzlich zulässigen Zeitraum wie folgt:

Der Beschwerde wird stattgegeben und festgestellt, dass die Beschwerdegegnerin die Beschwerdeführerin dadurch in ihrem Recht auf Geheimhaltung verletzte, indem sie deren personenbezogene Daten über einen zulässigen Zeitraum hinaus verarbeitete.

Der Beschwerdegegnerin wird aufgetragen, binnen einer Frist von zwei Wochen bei sonstiger Exekution

a) die Speicherung von Stammdaten der Beschwerdeführerin auf einen Zeitraum von höchstens sieben Jahren zu beschränken;

b) Verkehrsdaten der Beschwerdeführerin zu löschen;

c) alle personenbezogenen Daten der Beschwerdeführerin, welche keine Stamm- oder Verkehrsdaten sind, zu löschen.

Die Beschwerdegegnerin betreibt einen Telekommunikationsdienst. Zwischen der Beschwerdeführerin und der Beschwerdegegnerin bestand ein Vertragsverhältnis, welches September 2015 beendet wurde. Ein Auskunftsersuchen der Beschwerdeführerin im Frühjahr 2017 ergab, dass die Beschwerdegegnerin auch nach Beendigung des Vertragsverhältnisses gewisse Daten speichert. Die Beschwerdegegnerin speichert (neben weiteren personenbezogenen Daten, siehe nächsten Absatz) Stammdaten für die Dauer von 10 Jahren und Verkehrsdaten für die Dauer von 6 Monaten.

Gemäß Art. 5 Abs. 1 lit. e DSGVO müssen personenbezogene Daten in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer oder organisatorischer Maßnahmen, die von der DSGVO zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Art. 89 Abs. 1 verarbeitet werden („Speicherbegrenzung“) (*Hervorhebungen durch die Datenschutzbehörde*).

In der gegenständlichen Rechtssache stellt sich die Frage, ob eine längere Aufbewahrungsdauer der personenbezogenen Daten, auch über die Beendigung der Vertragsverhältnisse und somit über die Zweckerreichung hinaus, gerechtfertigt ist.

Zu den Stammdaten:

Gemäß § 97 Abs. 2 TKG 2003 sind Stammdaten spätestens nach Beendigung der vertraglichen Beziehungen mit dem Teilnehmer vom Betreiber zu löschen. Ausnahmen sind nur soweit zulässig, als diese Daten noch benötigt werden, um Entgelte zu verrechnen oder einzubringen, Beschwerden zu bearbeiten oder sonstige gesetzliche Verpflichtungen zu erfüllen.

Wenn sich die Beschwerdegegnerin bei der Speicherung von Stammdaten auf die zehnjährige Frist des § 207 Abs. 2 BAO beruft, so verkennt sie, dass hierbei lediglich eine Verjährungsfrist, jedoch keine konkrete Verpflichtung zur Aufbewahrung von Daten normiert wird. Eine gesetzliche Verpflichtung, Stammdaten über die Frist nach § 97 Abs. 2 TKG 2003 aufzubewahren, kann aus § 207 Abs. 2 BAO nicht abgeleitet werden. Auch der Verfassungsgerichtshof geht in seiner jüngeren Rechtsprechung davon aus, dass die weitere Aufbewahrung von Daten durch ein sich konkret abzeichnendes Verfahren gerechtfertigt sein muss. Die bloße Möglichkeit, dass ein Verfahren eingeleitet wird, reicht hingegen nicht aus (siehe dazu das Erkenntnis vom 12. Dezember 2017, GZ E3249/2016).

Anders verhält es sich mit § 132 Abs. 1 BAO, welcher eine Aufbewahrungspflicht von Büchern und Aufzeichnungen für sieben Jahren normiert und somit auch den datenschutzrechtlichen Vorgaben des Art. 5 Abs. 1 lit. e DSGVO bzw. von § 97 Abs. 2 TKG 2003 entspricht.

Die Beschwerdegegnerin ist daher befugt, Stammdaten gemäß § 132 Abs. 1 BAO für die Dauer von sieben Jahren aufzubewahren.

Zu den Verkehrsdaten:

Gemäß § 99 Abs. 2 TKG 2003 hat der Betreiber eines öffentlichen Kommunikationsnetzes oder –dienstes Verkehrsdaten zu speichern, sofern dies für Zwecke der Verrechnung von Endkunden- oder Vorleistungsentgelten erforderlich ist. Die Verkehrsdaten sind zu löschen oder zu anonymisieren, sobald der Bezahlvorgang durchgeführt wurde und innerhalb einer Frist von drei Monaten die Entgelte nicht schriftlich beeinsprucht wurden.

Die Datenschutzbehörde versteht zwar, dass die Beschwerdegegnerin im Hinblick auf den entsprechenden Postlauf bzw. interne Prozesse eine pauschale sechsmonatige Speicherdauer für Verkehrsdaten willkommen heißt, jedoch entspricht auch dies nicht den gesetzlichen Vorgaben des Art. 5 Abs. 1 lit. e DSGVO und stellt somit eine Verletzung des Grundrechtes auf Datenschutz dar.

3.2. Datenschutzbehörde (DSB) - Löschverpflichtung Gläubigerschutzverband und eventuell zukünftige Kontaktaufnahme kein berechtigtes Interesse (DSB-D216.580/0002- DSB/2018 am 28.05.2018 [Link]):

Die Datenschutzbehörde entscheidet über die Datenschutzbeschwerde des Andreas A*** (Be-schwerdeführer) vom 1. November 2017 gegen den N***-Gläubigerschutzverband (Beschwerdegegner) wegen Verletzung im Recht auf Löschung in Folge Weigerung des Beschwerdegegners personenbezogene Daten des Beschwerdeführers, welche im Zuge der Kommunikation erhoben wurden, zu löschen.

Der Beschwerdeführer begehrte am 6. Juli 2017 die Löschung seiner Daten aus der Datenbank des Beschwerdegegners. In weiterer Folge wurden dessen Daten zwar gelöscht und dies dem Beschwerdeführer mit Schreiben vom 27. Juli 2017 mitgeteilt, jedoch gab der Beschwerdegegner dem Beschwerdeführer gegenüber bekannt, dass eine erneute Speicherung seiner Daten (Vor- und Zuname, Geburtsdatum sowie aktuelle Adresse) zu Dokumentations- und Kommunikationszwecken erfolgte. Daraufhin begehrte der Beschwerdeführer die Löschung sämtlicher Daten, da zu einer Speicherung für Dokumentations- und Kommunikationszwecken keine Rechtsgrundlage bestehe. Dem erneuten Antrag auf Löschung wurde durch den Beschwerdegegner jedoch nicht entsprochen.

Insbesondere die Speicherung der Daten im Hinblick auf eine eventuell zukünftige Kontaktaufnahme mit dem Beschwerdeführer, wenn dieser die Löschung seiner gesamten Daten verlangt und daraus zu schließen ist, dass eine derartige Kommunikation nicht mehr erfolgen wird, ist gemäß Art. 17 Abs. 1 lit. a DSGVO nicht notwendig. Die zeitlich unbegrenzte Speicherung von personenbezogenen Daten für eine eventuell zukünftige Kontaktaufnahme stellt außerdem eine Verletzung des Grundsatzes der Speicherbegrenzung nach Art. 5 Abs.

1 lit. e DSGVO dar.

Andere, eine fortgesetzte Datenspeicherung rechtfertigende Gründe, wurden vom Beschwerdegegner nicht vorgebracht.

3.3. Oberster Gerichtshof (OGH) – kein „absolutes Koppelungsverbot“ (OGH 31.08.2018, 6 Ob 140/18h [Link]):

An die Beurteilung der „Freiwilligkeit“ einer datenschutzrechtlichen Einwilligung sind strenge Anforderungen zu stellen. Bei der Koppelung (a) der Einwilligung zu einer Verarbeitung (vertragsunabhängiger) personenbezogener Daten mit (b) einem Vertragsabschluss ist grundsätzlich davon auszugehen, dass die Erteilung der Einwilligung nicht freiwillig erfolgt, wenn nicht im Einzelfall besondere Umstände für eine Freiwilligkeit der datenschutzrechtlichen Einwilligung sprechen. (OGH 31.08.2018, 6 Ob 140/18h [Link])

GEISTWERT’s Schlussfolgerungen: Es gibt zwar kein „absolutes Koppelungsverbot“, doch muss derjenige, der sich auf die Zulässigkeit der „gekoppelten“ Einwilligung beruft, die besonderen Umstände im Einzelfall darlegen, die für eine (dennoch gegebene) Freiwilligkeit sprechen.

3.4. Datenschutzbehörde (DSB) - Auskunftsrecht und kostenlose Konto(teil)auszüge (DSB-D122.844/0006-DSB/2018 am 21.06.2018 [Link])

Mit Eingabe vom 22. Jänner 2018 rügte der Beschwerdeführer, dass er von der Beschwerdegegnerin Überweisungsnachweise der letzten fünf Jahre benötige und lediglich Überweisungsnachweise, welche nicht länger als ein Jahr zurückdatieren, einsehen könne. Daraufhin ersuchte der Beschwerdeführer die Beschwerdegegnerin um Übermittlung der Nachweise für die anderen Jahre. Die Beschwerdegegnerin hätte aber die Zurverfügungstellung der Überweisungsnachweise mit EUR 30,-- pro Jahr vergebührt. Der Beschwerdeführer hätte daraufhin ein datenschutzrechtliches Auskunftsbegehren gestellt und bis Ablauf der Frist keine Auskunft bekommen.

Gemäß § 69 DSG gibt es keine gesetzliche angeordnete Übergangsfrist und daher ist die Rechtslage im Zeitpunkt der behördlichen Entscheidung maßgeblich. Somit ist das seinerzeitige Begehren des Beschwerdeführers, welches sich auf die damals geltende Rechtslage des § 26 DSG 2000 stützte, nach dem nunmehr anwendbaren Recht auf Auskunft nach Art. 15 DSGVO zu beurteilen und dem ZaDiG 2018 gegenüberzustellen.

Die Beschwerde war schon deshalb berechtigt, weil die Beschwerdegegnerin unbestritten auf das datenschutzrechtliche Auskunftsbegehren nicht in der nach dem DSG bzw. der DSGVO vorgesehen Weise reagiert hatte. Bereits die Nichtreaktion auf ein Auskunftsbegehren stellt eine Verletzung im Recht auf Auskunft dar weshalb der Beschwerde stattzugeben war.

Der Beschwerdeführer behauptet darüber hinaus, die Beschwerdegegnerin habe ihn im Recht auf Auskunft dadurch verletzt, dass sie (nicht nachvollziehbare) Kosten an die Auskunft über gewisse Kontoauszüge knüpft.

Die DSGVO kann nicht dahingehend interpretiert werden, als regle sie die Betroffenenrechte

abschließend. Vielmehr regelt die DSGVO, ihrem Anwendungsbereich entsprechend, die Betroffenenrechte in allgemeiner Weise, wobei es nicht ausgeschlossen ist, dass in anderen Rechtsakten der Union speziellere Regelungen zu den Betroffenenrechten vorgesehen sind. Da im vorliegenden Fall das ZaDiG 2018 kein spezielles Auskunftsrecht normiert, kann dadurch auch auf das Recht zur allgemeinen datenschutzrechtlichen Auskunft über eigene Daten nicht beschränkt werden.

Dem Beschwerdeführer steht es zu, eine kostenlose Kopie der zu überprüfenden personenbezogenen Daten zu erhalten, wobei das Recht auf Erhalt einer Kopie die Rechte und Freiheiten anderer Personen nicht beeinträchtigen darf (Art. 15 Abs. 3 und 4 DSGVO). Der Beschwerdeführer kann das Recht auf Auskunft geltend machen, um die ihn betreffende Datenverarbeitung zu überprüfen. Da Zahlungsbelege üblicherweise weit mehr als personenbezogene Daten der betroffenen Person, in diesem Fall des Beschwerdeführers, beinhalten, kann das datenschutzrechtliche Auskunftsrecht auch nur so weit gehen, als, dass es dem Zweck der Überprüfung der Rechtmäßigkeit der Datenverarbeitung entspricht.

Die Beschwerdegegnerin hat daher den Beschwerdeführer betreffende personenbezogene Daten dem Auskunftsbegehren folgend, unter Berücksichtigung der Einschränkung des Art. 15 Abs. 4 DSGVO, offenzulegen.

GEISTWERT's Anmerkung: entgegen der – offensichtlich verkürzten – Berichterstattung über diesen rechtskräftigen besteigt, ergibt sich daraus nicht, dass Kontoauszüge jedenfalls kostenlos zu beauskunften sind, weil die DSB bewusst Einschränkungen vornahm, indem sie aussprach, dass Zahlungsbelege üblicherweise weit mehr als personenbezogene Daten der betroffenen Person beinhalten, aber nur diesbezüglich ein datenschutzrechtliches Auskunftsrecht besteht. Andererseits ist es natürlich ein enormer Aufwand, die personenbezogenen Daten von den sonstigen Daten der Kontoauszüge zu trennen.

3.5. Datenschutzbehörde (DSB) – datenschutzrechtliche Einwilligung muss freiwillig sein und ist von AGB / Mitgliedsantrag zu trennen (DSB-D213.642/0002-DSB/2018 am 31.07.2018 [Link])

Die Datenschutzbehörde entscheidet im Rahmen eines amtswegigen Prüfungsverfahrens gegen einen Automobilclub bezüglich datenschutzrechtlicher Einwilligung:

Der Automobilclub verschickte an seine Mitglieder Formulare zur Anwerbung von neuen Mitgliedern. Das Formular ist in zwei Teile untergliedert. Der erste Teil enthält personenbezogenen Daten des Mitglieds selbst, der zweite Teil ist mit „Ich werde neues Automobilclub Mitglied" betitelt und dient der Erfassung personenbezogener Daten neuer Mitglieder. Im zweiten Teil des Formulars befindet sich unter dem Abschnitt „Information und Datenschutz" folgende Passage (Format und Schriftbild nicht originalgetreu wiedergegeben):

„*Datenschutzrechtliche EINWILLIGUNG gemäß Artikel 6 Abs 1 lit a DSGVO zu Marketing-zwecken: Ich willige ein, dass der Automobilclub meine personenbezogenen Daten (Vorname, Familienname, Clubkartennummer, Adresse, Telefonnummer, E-Mail-Adresse) zum Zweck der Zusendung/Mitteilung von Informationen über neue Angebote, Produkte und Dienstleistungen wie insbesondere über Clubartikel.*

O per Post O per elektronischem Übermittlungsweg O per Telefon

verarbeitet und an die Landesvereine des Automobilclubs sowie die sonstigen Gesellschaften im Automobilclub-Verbund für diese Zwecke übermittelt. Die Nutzung der Daten zur Erbringung der Leistungen aus Mitgliedschaft ist von dieser Einwilligung unabhängig.

Widerruf: Diese Einwilligungen kann ich jederzeit per E-Mail an widerruf@automobilclub.at oder Brief widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der bis zum Widerruf erfolgten Verarbeitung nicht berührt."

Darunter befindet sich ein neuer Abschnitt, welcher für das gänzliche Formular gilt, mit einem Textfeld für Datum und Unterschrift. Da es sich um eine schriftliche Einwilligungserklärung handelt ist Art. 7 Abs. 2 Satz 1 DSGVO anwendbar und muss das Ersuchen um Einwilligung daher in verständlicher und leicht zugänglicher Form, in einer klaren und einfachen Sprache so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist. Gegenständlich ist die vorformulierte Einwilligungserklärung des Automobilclubs jedoch in einer Form aufgebaut, die der betroffenen Person den Eindruck vermittelt, lediglich entscheiden zu können durch welches Medium sie Marketing-Zusendungen erhalten möchte, nämlich per Post, per elektronischem Übermittlungsweg oder per Telefon.

Zudem trägt der allgemeine Aufbau des Formulars, konkret, die Platzierung der Einwilligungserklärung nach Art. 6 Abs. 1 lit. a DSGVO direkt vor der Unterschrift, welche die Anmeldung zur Mitgliedschaft bestätigt, zur weiteren Undeutlichkeit bei. Die betroffene Person kann die optionale Einwilligung der Verarbeitung von personenbezogenen Daten zu Marketingzwecken so als zwingenden Bestandteil des Formulars verstehen und annehmen, dass für die Mitgliedschaft auch die Einwilligung zu einer solchen Verarbeitung erforderlich ist, weil die Unterschrift der betroffenen Person erst nach dieser Textpassage gesetzt wird.

Auch durch den, im unmittelbaren textlichen Zusammenhang stehenden Hinweis auf die Widerrufsmöglichkeit wird der Eindruck vermittelt, einer Datenverarbeitung zu Marketingzwecken jedenfalls zustimmen zu müssen und erst durch die Möglichkeit eines Widerrufs eine Datenverarbeitung zu solchen Zwecken unterbinden zu können („opt-out"-Lösung, welche durch die DSGVO nicht gestattet ist.

Als Konsequenz dessen ist auch die Freiwilligkeit einer solch abgegebenen Einwilligung fraglich.

Da das gegenständliche Formular eine Auswahlmöglichkeit, ob die betroffene Person überhaupt in die Verarbeitung ihrer personenbezogenen Daten zum Marketingzwecken einwilligt oder nicht, nicht explizit enthält und durch die Platzierung der verfahrensgegenständlichen Textpassage vor dem Feld der Unterschrift suggeriert, dass die Unterschrift auch gleichzeitig eine Einwilligung nach Art. 6 Abs. 1 lit. a DSGVO darstellt, ist aus Sicht der Datenschutzbehörde auch das Element der Freiwilligkeit nicht gegeben.

3.6. <u>Datenschutzbehörde (DSB) – anonyme Daten bzw. Anonymisierung als mögliches Mittel zur Löschung bei unverhältnismäßigem Aufwand des Wiederherstellens des Personenbezugs</u>

(DSB-D123.270/0009-DSB/2018 am 05.12.2018 [Link]):

Die Datenschutzbehörde hat festgehalten, dass dem Verantwortlichen hinsichtlich der Mittel – also der vorgenommenen Art und Weise, wie eine Löschung durchgeführt wird – ein Auswahlermessen zusteht. Da die DSGVO auf Daten ohne Personenbezug keine Anwendung findet, ist die Entfernung des Personenbezugs (also die „Anonymisierung“) grundsätzlich ein mögliches Mittel, um einem Löschbegehren zu entsprechen. Dabei gilt jedoch ein strenger Maßstab, wonach sichergestellt sein muss, dass weder der Verantwortliche selbst, noch ein Dritter ohne unverhältnismäßigen Aufwand den Personenbezug wiederherstellen kann.

Zum Begriff „Anonymisierung“

Einleitend ist zu bemerken, dass der verbindliche Teil der DSGVO den seitens der Beschwerdegegnerin verwendeten Begriff der „Anonymisierung“ nicht kennt.

Lediglich in ErwGr 26 wird festgehalten, dass die DSGVO keine Anwendung auf anonymisierte Daten findet, worunter Informationen verstanden werden, „die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann“.

Zur Entfernung des Personenbezugs („Anonymisierung“) als Mittel zur Löschung

Eine Definition des Begriffs „Löschung von personenbezogenen Daten“ iSv Art. 17 Abs. 1 findet sich weder im verbindlichen Teil der DSGVO, noch in den ErwGr der Verordnung. Nach Art. 4 Z 2 sind das Löschen und die Vernichtung als alternative Formen der Verarbeitung angeführt („das Löschen oder die Vernichtung“), die nicht zwingend deckungsgleich sind. Daraus erhellt, dass eine Löschung nicht zwingend eine endgültige Vernichtung voraussetzt.

Daher steht dem Verantwortlichen hinsichtlich der Mittel – sohin der vorgenommenen Art und Weise der Löschung ein Auswahlermessen zu.

Die Entfernung des Personenbezugs („Anonymisierung“) von personenbezogenen Daten kann somit grundsätzlich ein mögliches Mittel zur Löschung iSv Art. 4 Z 2 iVm Art. 17 Abs. 1 DSGVO sein. Es muss jedoch sichergestellt werden, dass weder der Verantwortliche selbst, noch ein Dritter ohne unverhältnismäßigen Aufwand einen Personenbezug wiederherstellen kann.

Nur wenn der Verantwortliche die Daten im Ergebnis auf einer Ebene aggregiert, sodass keine Einzelereignisse mehr identifizierbar sind, kann der entstandene Datenbestand als anonym (also ohne Personenbezug) bezeichnet werden.

Eine Löschung liegt dann vor, wenn die Verarbeitung und Nutzung der personenbezogenen Daten einer betroffenen Person – so wie im vorliegenden Fall – nicht mehr möglich ist. Dass sich zu irgendeinem Zeitpunkt eine Rekonstruktion (etwa unter Verwendung neuer technischer Hilfsmittel) als möglich erweist, macht die „Löschung durch Unkenntlichmachung“ nicht unzureichend. Eine völlige Irreversibilität ist daher – unabhängig

vom verwendeten Mittel zur Löschung – nicht notwendig.

3.7. Datenschutzbehörde (DSB) – zur Unzulässigkeit von aktivierbaren Dash-Cams / Überwachungskameras im Straßenverkehr (auch) nach der DSGVO (DSB-D485.000/0001-DSB/2018-I am 09.07.2018 [Link]):

Die Datenschutzbehörde entscheidet aufgrund des von Dr. Tobias Q*** (Einschreiter) am 8.6.2018 eingeleiteten Verfahrens gemäß Art. 36 DSGVO betreffend eine beabsichtigte Verarbeitung von Daten (Aufnahme und kurzzeitige Speicherung von Videos mittels an der Frontscheibe eines Kfz angebrachter Videokamera) wie folgt:

Die Datenschutzbehörde spricht eine Warnung dahingehend aus, dass der genannte beabsichtigte Verarbeitungsvorgang voraussichtlich gegen die DSGVO verstößt.

Mit Schreiben vom 8.6.2018 hat der Einschreiter die Datenschutzbehörde gemäß Art. 36 DSGVO konsultiert, da aus der von ihm durchgeführten und übermittelten Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO hervorgehe, dass die von ihm beabsichtigte Verarbeitung von Daten (Aufnahme und kurzzeitige Speicherung von Videos mittels an der Frontscheibe eines Kfz angebrachter Videokamera) ein hohes Risiko zur Folge habe.

Konkret geht es im vorliegenden Fall darum, dass die angebrachte Videokamera ihre gemachten Aufnahmen in einem Intervall von 60 Sekunden laufend löscht. Dauerhaft gespeichert werden nur die 60 Sekunden vor und nach einem Unfall, welchen die Videokamera durch die Erschütterung des Unfalls und/oder durch Betätigung eines Notfall-Knopfes am Armaturenbrett erkennt.

Als Rechtfertigungsgrund gibt der Einschreiter in seiner Datenschutz-Folgenabschätzung an, dass die Verarbeitung der Daten zur Wahrung berechtigter Interessen des Verantwortlichen erfolgt.

Gemäß Art. 5 Abs. 1 lit. c DSGVO sehen auch die Grundsätze der DSGVO vor, dass personen-bezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein müssen („Datenminimierung“).

Nach dieser Bestimmung hat sohin eine Prüfung dahingehend stattzufinden, ob eine Beschränkung auf das für die Zwecke der Verarbeitung notwendige Maß erfolgt.

Dadurch, dass auch das Drücken des Notfall-Knopfes eine Speicherung der Bilddaten auslöst, kann nicht behauptet werden, dass eine Beschränkung auf das notwendige Maß beschränkt ist, zumal der Notfall-Knopf zu jedem beliebigen Zeitpunkt gedrückt werden könnte und somit eine dauerhafte Speicherung der Bilddaten auch ohne ein Unfallgeschehen erfolgen könnte.

Dem Erwägungsgrund 47 der DSGVO ist zu entnehmen, dass insbesondere dann, wenn personenbezogene Daten in Situationen verarbeitet werden, in denen eine betroffene Person vernünftigerweise nicht mit einer weiteren Verarbeitung rechnen muss, die Interessen und Grundrechte der betroffenen Person das Interesse des Verantwortlichen

überwiegen könnten. Insofern hätte für die Beurteilung der Frage der Rechtmäßigkeit der Verarbeitung im Sinne des Art. 6 Abs. 1 lit. f DSGVO eine Verhältnismäßigkeitsprüfung stattzufinden.

Personen, die am Straßenverkehr teilnehmen, müssen jedoch vernünftigerweise nicht damit rechnen, dass ihre personenbezogenen Daten, und dazu gehören unstrittig die mit der geplanten Verarbeitung im Zusammenhang stehenden, auf diese Weise verarbeitet werden. Es kann nämlich nicht behauptet werden, dass eine Speicherung von Bilddaten mithilfe von in Kfz angebrachter Videokameras heutzutage der gängigen Praxis im Straßenverkehr entspricht.

3.8. Bundesverwaltungsgericht (BVwG) – DSGVO sofort anwendbar und zum „Schikaneverbot" bzw „Auskunftsinteresse" iZm Betroffenenrechten (BVwG 27.09.2018, W214 2127449-1 [Link]):

Das Bundesverwaltungsgericht nimmt [Anmerkung: wie alle österreichischen Behörden] die sofortige Anwendbarkeit der DSGVO (auch auf vergangene Sachverhalte und anhängige Verfahren) an.

Die Rechtsanwältin, an die ein Prozessgegner ein datenschutzrechtliches Auskunftsbegehren gestellt hatte, wendete unter anderem schikanöse Rechtsausübung ein. Das BVwG erwog dazu: Dass eine Rechtsausübung für den Verpflichteten Belastungen mit sich bringt (was bei einer datenschutzrechtlichen Auskunftserteilung sicher der Fall ist) ist vom Gesetzgeber regelmäßig so gewollt. Um von Schikane sprechen zu können, muss das verpönte Motiv im einzelnen Fall nachgewiesen sein.

Ein pauschaler Verweis auf die anwaltliche Verschwiegenheitspflicht zur Verweigerung eines datenschutzrechtlichen Auskunftsbegehrens ist unzulässig. Es ist in der Verweigerung der Auskunft im Detail darzulegen, warum diese gemäß der Verschiedenheitspflichten nicht erteilt werden kann.

Die neue Rechtslage sieht auch keine strengeren Regelungen zur Identitätsfeststellung vor: Gemäß DSGVO kann der Verantwortliche, wenn er begründete Zweifel an der Identität der natürlichen Person, die den Antrag stellt, hat, zusätzliche Informationen anfordern, die zur Bestätigung der Identität der betroffenen Person erforderlich sind. Eine inhaltliche Auskunftsverweigerung kann damit nachträglich nicht begründet werden.

3.9. Bundesverwaltungsgericht (BVwG) – datenschutzrechtliche Rollenverteilung, hier: Des Gerichtssachverständigen (BVwG 27.09.2018, W214 2196366-2 [Link]):

Das Bundesverwaltungsgericht vertritt - in Abweichung von den Gesetzeserläuterungen - die Rechtsansicht, dass gerichtlich beeidete Sachverständige zumindest gemeinsam mit dem Gericht, das sie mit der Gutachtenserstellung beauftragt hat, als datenschutzrechtliche Verantwortliche zu betrachten sind, da sie selbständig und eigenverantwortlich über die Mittel ("Art und Weise, wie ein Ergebnis oder Ziel erreicht wird") entscheiden. Das Gericht hat hinsichtlich der Methodik der Gutachtenserstellung und der Entscheidung, welche personenbezogenen Daten konkret verarbeitet werden, keinerlei Einfluss auf den Inhalt des Gutachtens und auch keine diesbezüglichen Weisungsbefugnisse. Damit wird von den Sachverständigen über wesentliche Aspekte der Mittel selbst entschieden.

GEISTWERT's Kritik: Die Rollenverteilung ist eines der heikelsten Themen des Datenschutzrechts: Sie Ausgangspunkt für zahllose Konsequenzen. Diese Rollenverteilung wird uns wohl noch länger begleiten, bis Klarheit besteht. Gemäß DSGVO ist „Verantwortlicher", wer „[…] *allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet;* […]". Diese UND-Verknüpfung bedeutet uE, dass beide Voraussetzungen zumindest ansatzweise gegeben sein müssen bzw „Mittel" auch den bloßen Umstand des Einsatzes eines Auftragsverarbeiters umfasst: hier, dass das Gericht einen Sachverständigen zu Gutachtenserstellung (= „Zweck" und legt damit auch den Umfang im Sinne von „Mittel" fest) beauftragt. Das von der europäischen Datenschutzgruppe (nunmehr: Europäischer Datenschutzausschuss) erstellte WP 169[1] sieht dies – entgegen der Ansicht des BVwG – wohl ähnlich, wenn es ausführt: „[…] *Da es sich um ein Begriffspaar handelt, wäre zu klären, wie stark der Einfluss auf das „Warum" und das „Wie" sein muss, um als für die Verarbeitung Verantwortlicher zu gelten.* […] *Anders ausgedrückt bezeichnet der Begriff „Mittel" nicht nur die technischen Methoden für die Verarbeitung personenbezogener Daten, sondern auch das „Wie" der Verarbeitung; dazu gehören Fragen wie „Welche Daten werden verarbeitet?", „Welche Dritte haben Zugang zu diesen Daten?", „Wann werden Daten gelöscht?" usw. Die Entscheidung über die „Mittel" beinhaltet daher einerseits technische und organisatorische Fragen, deren Entscheidung problemlos an Auftragsverarbeiter delegiert werden kann (wie z. B. „Welche Hardware oder Software wird verwendet?"), und andererseits wesentliche Elemente, die traditionell und naturgemäß der Entscheidung durch den für die Verarbeitung Verantwortlichen vorbehalten sind, wie z. B. „Welche Daten werden verarbeitet?", „Wie lange werden sie verarbeitet?", Wer hat Zugang zu ihnen?" usw.* […]. *Vor diesem Hintergrund ist es durchaus möglich, dass ausschließlich der Auftragsverarbeiter über die technischen und organisatorischen Mittel entscheidet.*" Da die Gerichtssachverständigen hinsichtlich des Zwecks und des sich daraus ergebenden Umfang der Datenverarbeitung an den Gutachtensauftrag gebunden sind, entscheiden die Gerichtssachverständigen tatsächlich nur im Rahmen dessen über die Frage, welche Daten konkret verarbeitet werden und über die technischen Mittel. Aufgrund dieser Beschränkung sind die Gerichtssachverständigen zwanglos als Auftragsverarbeiter zu qualifizieren. Folgt man hingegen der Ansicht des BVwG führt dies zu praktisch absurden Konsequenzen, insbesondere könnten über die datenschutzrechtlichen Betroffenenrechte gegenüber den Gerichtssachverständigen die prozessgesetzlichen Regelungen zur Akteneinsicht usw ausgehebelt werden.

3.10. Landesverwaltungsgericht Tirol (T-LVwG) – DSG schützt auch nach DSGVO bzw Novelle juristische Personen (LVwG-2018/29/0312-5 vom 02.11.2018 [Link])

Die Tiroler Landesregierung hat im Verfahren vor dem T-LVwG (ua) umfassend zur Frage argumentiert, ob das DSG auch nach der DSGVO bzw. nach der Novelle 2018 den Schutz der Daten von juristischen Personen (noch) in sich begreift. Das T-LVwG sprach dann als Beschwerdegericht kurz und trocken aus: „*Insofern besteht auch im Sinne des § 1 DSG – welcher nach wie vor für juristische Personen in Geltung ist – ein entsprechendes schutzwürdiges Interesse an der Geheimhaltung* […]*."*

[1] http://www.privacy-regulation.eu/privazyplan/article29/files/wp169%20DE%20Verantwortlicher%20vs.%20Auftragsverarbeiter%202010%2002%2016.pdf.

Vgl dazu oben zur „Novelle 2019“.

3.11. Datenschutzbehörde (DSB) – Einwilligung und Widerruf bei Cookies, Bezahl-Abo-Alternative und Widerspruch # Widerruf (DSB-D122.931/0003-DSB/2018 vom 30.11.2018 [Link]):

Aus Sicht der Datenschutzbehörde geht die ePrivacy-RL bzw. das TKG 2003 (Anmerkung: vgl Novelle des TKG im BGBl vom 30.11.2018 [Link]) dem DSG bzw. dem DSGVO als *lex specialis* vor.

Zum Anlassfall ist zunächst zu bemerken, dass die Beschwerdegegnerin bei Einwilligung zur Nutzung der Webpage (Variante 1) solange keine Cookies setzt, bis der Besucher der Webpage eine bewusste Entscheidung getroffen, also eine Einwilligung abgegeben hat, ob er Variante 1 in Anspruch nehmen möchte. Durch Verlinkung im Fenster („Pop-Up“) auf die Datenschutzerklärung und durch eine Aufzählung der im Einsatz befindlichen Cookies („Cookies-Anhang“) entspricht die Beschwerdegegnerin auch der in gesetzlich geforderten transparenten Informationspflicht und ist auch ein eindeutiger und bestimmter Zweck ersichtlich, wodurch für die betroffene Person eine Kontrolle hinsichtlich der Verarbeitung ihrer Daten sichergestellt ist. Gibt eine betroffene Person keine Einwilligung ab, so besteht die erste Konsequenz darin, dass diese ein O**-Abo abschließen kann. Dieses O**-Abo ist – wie festgestellt – frei von Werbung, frei von Daten-Tracking und frei von der Setzung von Fremdcookies. Das O**-Abo ist mit einem Preis von 6 Euro monatlich ab dem zweiten Monat auch keine unverhältnismäßig teure Alternative. Die zweite Konsequenz bei Nichtabgabe einer Einwilligung besteht darin, dass die betroffene Person die Webpage der Beschwerdegegnerin nicht in Anspruch nimmt und auf ein alternatives Informationsangebot zurückgreift. Im Ergebnis liegt in den Konsequenzen bei Nichtabgabe einer Einwilligung bei weitem kein wesentlicher Nachteil vor und ist die betroffene Person mit keinen beträchtlichen negativen Folgen konfrontiert.

GEISTWERT’s Schlussfolgerungen: Die DSB spricht in diesem (nicht rechtskräftigen) Bescheid wesentliche Fragestellungen der Praxis an: Neben der Klarstellung des Verhältnisses zwischen TKG und DSGVO wird ausgesprochen, dass (entgeltliche) Alternativen eine Koppelung von zwingender Einwilligung zur Nutzung zulässig machen kann (kein „absolutes Koppelungsverbot“). Interessant ist, dass die DSB einen (fälschlich erhobenen) Widerspruch nicht zum Widerruf „uminterpretiert“ hat. Auch dass von der DSB anerkannt wird, dass der Widerruf bei Cookies auch durch entsprechende Einstellungen im Browser bzw. durch Löschen sämtlicher oder einzelner Cookies in den Browsereinstellungen erfolgen kann, zeigt hohes praktisches Verständnis.

3.12. Datenschutzbehörde (DSB) – keine Geltendmachung zukünftiger Verletzungen und spezifischer Datensicherheitsmaßnahmen (DSB-D123.070/0005-DSB/2018 vom 13.9.2018 [Link]):

Die Datenschutzbehörde kann eine Verletzung des Grundrechts auf Geheimhaltung nur *ex post* feststellen, weshalb die Beschwerde hinsichtlich möglicherweise in Zukunft eintretender Verletzungen abzuweisen war.

Hinsichtlich einer Verletzung des Grundrechts auf Geheimhaltung durch eine „unterlassene Pseudonymisierung“ ist festzuhalten, dass aus der DSGVO kein Recht abzuleiten ist, wonach eine betroffene Person spezifische Datensicherheitsmaßnahmen iSd DSGVO von

einem Verantwortlichen verlangen könnte. Ebenso wenig kann eine betroffene Person spezifische Maßnahmen zur Datenminimierung verlangen.

3.13. Datenschutzbehörde (DSB) – zu Löschpflicht und Löschkonzepten, *in concreto* Bewerbungsunterlagen (DSB-D123.085/0003-DSB/2018 vom 27.8.2018 [Link]):

Das Recht auf Löschung gemäß DSGVO kommt dann nicht in Betracht, wenn eine Verarbeitung in den von Art. 17 Abs. 3 lit a bis e DSGVO taxativ aufgezählten Fällen erforderlich ist. Der Tatbestand „Verteidigung von Rechtsansprüchen" greift in zeitlicher Hinsicht jedenfalls dann, wenn die Geltendmachung, Ausübung oder Verteidigung von (bzw. gegen) Rechtsansprüchen schon stattfindet oder sicher bevorsteht; die bloß abstrakte Möglichkeit rechtlicher Auseinandersetzungen ist hingegen nicht ausreichend.

Im vorliegenden Fall verweigerte die Beschwerdegegnerin – zumindest vorerst – die sofortige Löschung der Bewerberdaten des Beschwerdeführers und führte eine mögliche Geltendmachung eines Ersatzanspruches nach § 26 Abs. 1 GlBG ins Treffen. Nach § 29 Abs. 1 GlBG kann ein Ersatzanspruch innerhalb einer Frist von sechs Monaten geltend gemacht werden. Die Beschwerdegegnerin bezieht sich somit nicht allgemein auf ein potenziell zukünftiges Verfahren, sondern benennt einen konkreten Anspruch, der ihr gegenüber innerhalb eines konkreten Zeitraumes geltend gemacht werden könnte.

Darüber hinaus erklärte sich die Beschwerdegegnerin aber bereit, die Bewerberdaten des Beschwerdeführers zum ehest möglichen Zeitpunkt zu löschen, also nach Ablauf der Frist. Der zusätzlich berechnete Monat zu der sechsmonatigen Frist, um einen potenziellen Klageweg einzuberechnen, ist angemessen und nicht unverhältnismäßig lange.

GEISTWERT's Schlussfolgerungen: Löschkonzepte – also wann welche Datenkategorien gelöscht werden, im Idealfall auch unter Berücksichtigung des „Wie sie gelöscht werden" – sind in den meisten Datenschutzprojekten eine der größten Herausforderungen, weil die grundsätzliche Löschverpflichtung durch zahllose Aufbewahrungspflichten „durchbrochen" wird und – wie der Bescheid hinsichtlich des zusätzlichen Monats zeigt – die Löschverpflichtung auch gegen berechtigte Interessen abzuwägen ist. Die DSB hat hinsichtlich Letzterem begrüßenswerter Weise im Bescheid einen praxisnahen Zugang gewählt.

3.14. Datenschutzbehörde (DSB) - Durchsetzung des Auskunftsanspruchs setzt ein Auskunftsbegehren vor Einleitung des Verfahrens voraus / Hausmeister ist keine Abgabestelle (DSB-D123.512/0004-DSB/2018 vom 11.01.2019 [Link])

Die Datenschutzbehörde entscheidet über die Datenschutzbeschwerde von Herrn Karl A*** (Beschwerdeführer) vom 17. September 2018 gegen die Stadt N***, **** Wohnhausverwaltung (Beschwerdegegnerin) wegen Verletzung im Recht auf Auskunft wie folgt:

- Die Beschwerde wird abgewiesen.

In seiner verfahrenseinleitenden Eingabe vom 17. September 2018 führte der Beschwerdeführer aus, die Beschwerdegegnerin habe ihn im Recht auf Auskunft verletzt, indem sie auf seinen Antrag gemäß § 44 DSG vom 17. Juli 2018 nicht geantwortet habe.

Der Beschwerdeführer führte dazu aus, er habe das Auskunftsbegehren bei „der Erfüllungsgehilfin Hausbesorger U***“ abgegeben und sei dadurch auch seine Identität geklärt.

Der Beschwerdeführer meint, sein Auskunftsbegehren schon dadurch wirksam gestellt zu haben, indem er es in den Briefkasten der Dienstwohnung der Hausbesorgerin als „Erfüllungsgehilfin“ der Beschwerdegegnerin eingeworfen hat. Dem ist im Ergebnis nicht zu folgen:

Der Beschwerdeführer behauptet eine Verletzung im Recht auf Auskunft, ohne ein den Verfahrens¬gegenstand bildendes Auskunftsbegehren wirksam gestellt zu haben. Das Auskunftsbegehren hat nämlich die Beschwerdegegnerin nie erreicht. Der Beschwerdeführer hat im laufenden Verfahren der Ausführung der Beschwerdegegnerin, dass diese das Auskunftsersuchen nicht erhalten hat, nicht bestritten. Er führte, auf Vorhalt durch die Datenschutzbehörde lediglich aus, dass er die Zustellung als „rechtlich erachte“, weil er es in das Postfach der Hausbesorgerin einwarf. Im Ergebnis meint der Beschwerdeführer, dass sein Anbringen schon dadurch in den Verfügungsbereich der Beschwerdegegnerin gelangte, weil er es in den Briefkasten der Dienstwohnung der Hausbesorgerin einwarf.

Dabei besteht kein Grund zur Annahme, die (gemäß §§ 3 und 4 Hausbesorgergesetz determinierten) Aufgaben der Hausbesorger würden auch die Entgegennahme und Weiterleitung von Schriftstücken beinhalten. Allein weil zwischen der Hausbesorgerin und der Beschwerdegegnerin ein Dienstvertrag besteht, deren wechselseitigen Pflichten keineswegs auf die Besorgung dieser Art von Aufgaben gerichtet ist, kann nicht geschlossen werden, dass ein Schriftstück in den Verfügungsbereich der Beschwerdegegnerin kam.

Ein Verantwortlicher (die Beschwerdegegnerin) hat gemäß Art. 12 DSGVO die Möglichkeit einer transparenten Kommunikation zur Verfügung zu stellen und darüber zu informieren. Dafür hält die Beschwerdegegnerin auf ihrer Webseite auch ein Kontaktformular betreffend datenschutzrechtliche Eingaben – neben dem allgemeinen Briefpostfach – bereit. Der Beschwerdeführer verwendete die zur Verfügung stehenden Kontaktmöglichkeiten aber nicht.

Art. 15 DSGVO ist konzeptionell ein antragbedürftiges Recht und bedarf a limine ein an den be-zeichneten Beschwerdegegner zugegangenes Begehren.

Nach der hg. Rechtsprechung zu behebbaren bzw. unbehebbaren Mängeln ist zu unterscheiden, ob im maßgeblichen Zeitpunkt der nachzuweisende Umstand fehlt (dies Falls liegt ein nicht behebbarer Mangel vor) oder ob es bloß am Nachweis des bereits bestehenden Umstandes mangelt (im letztgenannten Fall ist der Mangel behebbar.

Da das datenschutzrechtliche Auskunftsbegehren nie den bezeichneten Beschwerdegegner erreicht hat, fehlt es dem Beschwerdeführer in Bezug auf den gerügten Sachverhalt im Zeitpunkt der Einbringung der Beschwerde an der Legitimation.

3.15. Datenschutzbehörde (DSB) – Verstoß gegen das Spamming-Verbot / Verbot von Werbe-E-Mails nach TKG auch Datenschutzverstoß (DSB-D130.033/0003-DSB/2019 am 07.03.2019 [Link])

Die Datenschutzbehörde entscheidet über die Datenschutzbeschwerde von Dr. Ulrich A*** (Beschwerdeführer) vom 23. Juli 2018 gegen die N***, Inc (Beschwerdegegnerin), niedergelassen in CA 9*3*2 T***, USA, in der Union vertreten durch die N*** Nederland B.V., niedergelassen in **** Amsterdam, Niederlande, wegen Verletzung im Grundrecht auf Datenschutz wie folgt:

- Der Beschwerde wird stattgegeben und es wird festgestellt, dass die Beschwerdegegnerin den Beschwerdeführer dadurch im Grundrecht auf Datenschutz verletzt hat, indem sie an diesen am 19. Juli 2018 eine E-Mail zu Werbezwecken verschickt hat, obwohl keine Einwilligung hierzu vorlag.

Im vorliegenden Fall verschickte die Beschwerdegegnerin eine E-Mail zu Werbezwecken an den Beschwerdeführer, obwohl hierzu keine entsprechende Einwilligung eingeholt wurde.

Dazu ist festzuhalten, dass die Zusendung von elektronischer Post zu Werbezwecken ohne vorherige Einwilligung des Teilnehmers („Unerbetene Nachrichten“) nach der Bestimmung von § 107 Abs. 1 TKG 2003 (die Art. 13 Abs. 1 der Richtlinie 2002/58/EG, die „e-Datenschutz-RL“, umsetzt) zu beurteilen ist. Diesbezüglich hat sich die Rechtslage auch mit Geltung der DSGVO seit 25. Mai 2018 nicht verändert (vgl. Art. 95 DSGVO, wonach die Verordnung natürlichen oder juristischen Personen in Bezug auf die Verarbeitung in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Union keine zusätzlichen Pflichten auferlegt, soweit sie besonderen in der e-Datenschutz-RL festgelegten Pflichten unterliegen, die dasselbe Ziel verfolgen).

Dies bedeutet jedoch nicht, dass dem Beschwerdeführer keine Datenschutzbeschwerde gemäß Art. 77 Abs. 1 DSGVO zusteht. Zwar richtet sich die Zulässigkeit einer Kontaktaufnahme zu Werbezwecken - wie dargelegt - nach den Bestimmungen des TKG 2003 bzw. der e-Datenschutz-RL und nicht nach Art. 6 DSGVO. Jedoch kann durch einen Verstoß gegen das TKG 2003 bzw. die e-Datenschutz-RL gleichzeitig eine Verletzung des Rechts auf Geheimhaltung nach § 1 Abs. 1 DSG und auch eine Verletzung jener Bestimmungen der DSGVO vorliegen, die dem Verantwortlichen keine zusätzlichen Pflichten iSv Art. 95 DSGVO auferlegen.

Zum verletzt erachteten Recht:

Zunächst ist festzuhalten, dass sich der Beschwerdeführer in seinem Vorbringen zwar auf eine Verletzung der Art. 5 und Art. 6 DSGVO (sohin eine fehlende Einwilligung) stützte, die Betroffenenrechte jedoch in Kapitel III DSGVO (Art. 12 bis 23) taxativ aufgezählt werden.

Nach Rechtsprechung der Datenschutzbehörde kann sich eine betroffene Person dem Grunde nach trotzdem auf jede Bestimmung abseits von Kapitel III der DSGVO stützen, sofern dies im Ergebnis zu einer denkmöglichen Verletzung des Rechts auf Geheimhaltung nach § 1 Abs. 1 DSG führen kann.

Dementsprechend war eine Verletzung des Rechts auf Geheimhaltung zu überprüfen, das – wie dargelegt – nicht von Art. 95 DSGVO umfasst ist.

Wie bereits oben ausgeführt, richtet sich die Rechtmäßigkeit der Verarbeitung ausschließlich

nach der e-Datenschutz-RL als lex specialis.

Nach Art. 13 Abs. 1 der e-Datenschutz-RL ist vor dem Versand von elektronischer Post eine Einwilligung der betroffenen Person einzuholen. Zu bemerken ist jedoch, dass die e-Datenschutz-RL keine näheren Bedingungen bzw. keine Definition für die Einwilligung vorsieht.

Allerdings verweist die e-Datenschutz-RL hinsichtlich des Begriffes der „Einwilligung“ auf die Einwilligung im Sinne der Richtlinie 95/46/EG (Datenschutz-Richtlinie; vgl. dazu Art. 2 lit. f e Datenschutz-RL). Der Begriff der Einwilligung nach der e-Datenschutz-RL entspricht daher in systematischer Auslegung dem Begriff der Einwilligung nach Art. 4 Z 11 bzw. Art. 7 DSGVO, wie sich aus Art. 94 Abs. 2 DSGVO ergibt.

Die Verarbeitung kann daher nicht auf einen alternativen Erlaubnistatbestand nach Art. 6 DSGVO (etwa berechtigte Interessen nach Abs. 1 lit. f leg. cit.) gestützt werden, was die Beschwerdegegnerin auch nicht behauptet hat.

Da jedoch, wie festgestellt, keine Einwilligung für den Erhalt von E-Mails zu Werbezwecken vorlag, wurden die personenbezogenen Daten des Beschwerdeführers (seine E-Mail-Adresse mit Klarnamen) unrechtmäßig (d.h. ohne Erlaubnistatbestand) verarbeitet, weshalb eine Verletzung von § 1 Abs. 1 DSG iVm Art. 8 Abs. 1 EU-GRC vorliegt.

Da der Beschwerdeführer - trotz Ersuchens der Beschwerdegegnerin mit E-Mail vom 18. Mai 2018 - keine entsprechende Einwilligung mehr abgegeben hat, wäre die Beschwerdegegnerin dazu verpflichtet gewesen, die E-Mail-Adresse des Beschwerdeführers zu löschen; allerdings ist darauf hinzuweisen, dass sich diese Verpflichtung nicht erst aus der DSGVO ergibt, sondern bereits nach alter Rechtslage gemäß der Datenschutz-Richtlinie bestanden hat.

Da die Beschwerdegegnerin bereits mit Stellungnahme vom 13. Februar 2019 angab, dass die E-Mail-Adresse des Beschwerdeführers von „allen zukünftigen Marketing-Mitteilungen von N*** vollständig entfernt“ worden sei, war kein Leistungsauftrag gemäß § 24 Abs. 5 DSG bzw. Art. 58 Abs. 2 lit. c DSGVO zu erteilen.

3.16. Datenschutzbehörde (DSB) – „Informationsfreiheitsprivileg“ nach § 9 DSG (DSB-D123.077/0003-DSB/2018 vom 13.8.2018 [Link]):

§ 9 DSG knüpft an Art. 85 DSGVO an; man kann daher von einem datenschutzrechtlichen „Informationsfreiheitsprivileg“ (in Folge nur: „Privileg“) sprechen.

Im vorliegenden Fall stellt die Beschwerdegegnerin Artikel zu diversen Themen online. Diese Artikel fallen unstrittig unter das Privileg. Zu überprüfen ist jedoch, ob auch der Diskurs zwischen Benutzern im Online-Forum - also die Postings der Benutzer unterhalb der Artikel - vom Privileg erfasst ist. Die Postings bzw. der Inhalt der Postings lassen sich auf den Beschwerdeführer zurückführen.

Der nationale Gesetzgeber beschränkt das Privileg, indem es nur Medienunternehmen oder Mediendiensten zugänglich ist. Um der Bedeutung des Rechts auf freie Meinungsäußerung in einer demokratischen Gesellschaft Rechnung zu tragen, müssen aber Begriffe wie

Journalismus, die sich auf diese Freiheit beziehen, nach Ansicht der DSB im Ergebnis weit ausgelegt werden. Vor diesem Hintergrund muss das Privileg ausgelegt werden und kann im Lichte der Rechtsprechung des EuGH auch „Bürgerjournalismus“ umfassen (bspw. Internet-Diskussionsforen), der den Zweck der einseitigen oder wechselseitigen Kommunikation von Ideen, Meinungen und Informationen verfolgt.

3.17. Datenschutzbehörde (DSB) – Genehmigung zu Forschungszwecken nach § 7 DSG (DSB-D202.208/0001-DSB/2018 vom 3.8.2018 [Link]):

Die Genehmigung iSd § 7 Abs. 3 DSG bezieht sich (im gegenständlichen Fall) nur auf Datenverarbeitungen zur Erreichung des historischen Forschungszweckes, in diesem Fall der Erarbeitung einer Ortschronik der Gemeinde P*berg bei T*kirchen. Die Datenschutzbehörde kann demnach nur Datenverarbeitungen genehmigen, die dem historischen Forschungszweck dienen. Ist dieser erreicht, so sind weitere Datenverarbeitungen nicht nach der Sondervorschrift des § 7 DSG zu beurteilen, sondern unterliegen den allgemeinen Zulässigkeitsvoraussetzungen der DSGVO. Das betrifft in diesem Fall all jene Datenverarbeitungen, die nach Erarbeitung der Ortschronik erfolgen (insbesondere die Übermittlung der Ortschronik an die Gemeinde P*berg bzw. die Veröffentlichung derselben bei der Jubiläumsfeier). Hiernach hat der Verantwortliche selbst nach der DSGVO zu beurteilen, ob die jeweiligen Datenverarbeitungen zulässig sind.

3.18. Oberster Gerichtshof (OGH) – Akteneinsicht und Verwendung von Gesundheitsdaten aus Zivilprozess für Strafverfahren (OGH 24.07.2019, 6Ob45/19i [Link]):

Die Kläger begehrten von der beklagten Spitalserhalterin Schadenersatz wegen medizinischen Behandlungsfehlern an der Klägerin und ihrem verstorbenen Kind im Zuge der Entbindung. Mit Schriftsatz vom 18. 6. 2018 stellte die Hebamme den Antrag auf Akteneinsicht und Übermittlung des Urteils sowie der Beschlüsse, Protokolle und Gutachten gegen Kostenbekanntgabe. Sie begründete ihr rechtliches Interesse mit einem gegen sie als diensthabender Hebamme geführten Strafverfahren im Zusammenhang mit der Entbindung des Kindes der Klägerin. Die Kläger und die Beklagte sprachen sich gegen die Gewährung von Akteneinsicht aus.

Das Recht auf Akteneinsicht im Zivilprozess ist in § 219 ZPO geregelt. Die Gewährung von Akteneinsicht durch das Gericht ist allerdings gleichzeitig als Verarbeitung im Sinn der Legaldefinition des Art 4 Z 2 DSGVO zu qualifizieren („Offenlegung durch Übermittlung“), sofern sie im Zusammenhang mit „personenbezogenen Daten“ im Sinn des Art 4 Z 1 DSGVO steht. Die DSGVO ist daher auf die Gewährung von Akteneinsicht durch ein österreichisches Gericht anzuwenden, wenn die Akteneinsicht Informationen umfasst, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (vgl Art 4 Z 1 DSGVO).

Liegt ein rechtliches Interesse zur Akteneinsicht vor, ist in einem nächsten Schritt die Abwägung vorzunehmen, ob das Interesse des Antragstellers gegenüber dem Geheimhaltungsinteresse eines anderen – auch einer nicht als Partei beteiligten Person – bzw gegenüber öffentlichen Interessen überwiegt. Dabei ist zu berücksichtigen, dass § 219 Abs 2 ZPO allgemein das Recht auf Datenschutz, Familien- und Privatleben schützt. Das Recht auf Datenschutz ist daher bei der Beurteilung gemäß § 219 ZPO zu beachten. Ist der Schutz personenbezogener Daten einer natürlichen Person betroffen, ist konkret auf den

von der DSGVO gewährten Schutzumfang abzustellen.

Gemäß Art 9 Abs 1 DSGVO ist die Verarbeitung von Gesundheitsdaten grundsätzlich untersagt. Gemäß Art 9 Abs 2 lit f DSGVO gilt das Verarbeitungsverbot des Abs 1 jedoch in jenen Fällen nicht, in denen die Verarbeitung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der Gerichte im Rahmen ihrer justiziellen Tätigkeit erforderlich ist. „Erforderlich" bedeutet, dass ohne die Daten die Geltendmachung des Anspruchs bzw eine Verteidigung dagegen nicht möglich oder wesentlich erschwert wäre. Die Grenze der „Erforderlichkeit" im Sinn des Art 9 Abs 2 lit f DSGVO ist aufgrund ihrer Bedeutung für die rechtsstaatliche Durchsetzung von Ansprüchen nicht allzu streng zu handhaben

Im vorliegenden Fall, in dem die strittige Akteneinsicht Gesundheitsdaten der Erstklägerin betrifft, hängt die Berechtigung des Einsichtsbegehrens daher davon ab, ob sich die Antragstellerin auf ein rechtliches Interesse stützt, das einem der Tatbestände des § 9 Abs 2 DSGVO entspricht, konkret, ob die begehrte Einsicht „zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen [der Antragstellerin] erforderlich" ist. Ist diese Frage zu bejahen, ist das Interesse der Antragstellerin gegen die Geheimhaltungsinteressen der Erstklägerin abzuwägen (Art 6 Abs 1 lit f DSGVO).

Hier ist die Einsicht der Antragstellerin in die im Zivilprozess erstatteten medizinischen Sachverständigengutachten sowie in die darauf bezüglichen Erörterungen für ihre Verteidigung in dem infolge der Entbindung des Kindes der Erstklägerin gegen die Antragstellerin geführten Strafverfahren erforderlich. Es liegt auf der Hand, dass die Verteidigung des Rechtsguts der Unbescholtenheit zumindest ebenso schwer wiegt wie die Verteidigung gegen allfällige vermögensrechtliche Ansprüche. Schon aus diesem Grund kann Art 9 Abs 2 lit f DSGVO nicht dahin ausgelegt werden, dass zwar die Abwehr von Schadenersatzansprüchen aus Behandlungsfehlern als Hebamme als „Abwehr von Rechtsansprüchen" eine Ausnahme vom Verbot der Bearbeitung der Gesundheitsdaten der Erstklägerin rechtfertigen könnte, nicht aber die Verteidigung in einem auf dasselbe Fehlverhalten gestützten Strafverfahren.

3.19. Verwaltungsgerichtshof (VwGH) – Geheimhaltungsanspruch unabhängig von den technisch-organisatorischen Bedingungen (VwGH 28.02.2018, Ra 2015/04/0087 [Link]):

§ 1 Abs 1 DSG 2000 gewährt einen umfassenden Geheimhaltungsanspruch personenbezogener Daten, unabhängig von den technisch-organisatorischen Bedingungen ihrer Verarbeitung, also auch bei nicht-automationsunterstützt verarbeiteten Daten.

GEISTWERT's Schlussfolgerungen - auch für die neue Rechtslage: § 1 DSG ist ja identisch Rechtsbestand im (neuen) DSG geblieben. Ob die durch den VwGH vorgenommene „Ausweitung" des Datenschutzrechts auf alle personenbezogene Daten unabhängig von den technisch-organisatorischen Bedingungen zu einem umfassenden Geheimhaltungsrecht unionsrechtlich zulässig ist, wird aber wohl schlussendlich der Europäische Gerichtshof (EuGH) zu prüfen und zu entscheiden haben.

3.20. Verwaltungsgerichtshof (VwGH) – Gesetzwidrigkeit *ähnlich* „unrechtmäßige Weise" (VwGH 26.06.2018, Ra 2017/04/0032 [Link]):

Für die Beurteilung der Rechtswidrigkeit einer Datenverarbeitung (noch nach alter Rechtslage) sind auch Regelungen außerhalb des Datenschutzrechts maßgeblich, soweit sie ihrerseits das Verbot einer (bestimmten Art der) Datenverwendung zum Inhalt haben. Aus der rechtswidrigen Ermittlung von Daten folgt auch die Rechtswidrigkeit einer daran anschließenden Übermittlung dieser Daten.

GEISTWERT's Schlussfolgerungen - auch für die neue Rechtslage: (i) Gesetzesverstöße außerhalb des Datenschutzrechts führen nur dann zum Automatismus, dass die Verarbeitung entgegen der DSGVO nicht auf rechtmäßige Weise erfolgt (Art 5 DSGVO), soweit das Gesetz seinerseits das Verbot einer (bestimmten Art der) Datenverarbeitung zum Inhalt hat. (ii) „Einmal unrechtmäßige … immer unrechtmäßige Verarbeitung": Auch über „Übermittlungsketten" odgl. kann eine einmal rechtswidrige Verarbeitung nicht „geheilt" werden.

3.21. Verwaltungsgerichtshof (VwGH) – Ermessen bei Strafe, aber Pflicht zur Nachvollziehbarkeit (VwGH 16.05.2018, Ra 2017/04/0080 [Link]):

Das DSG 2000 hat der Datenschutzbehörde hinsichtlich der Wahl des Strafmittels (weites) Ermessen eingeräumt, doch bedarf es bei der Ermessensübung nachvollziehbarer Darlegungen, die dem VwGH eine (wenn auch nur eingeschränkt erfolgende) Überprüfung dahin, ob das Ermessen im Sinn des Gesetzes ausgeübt wurde, ermöglichen.

GEISTWERT's Schlussfolgerungen - auch für die neue Rechtslage: (i) Viel mediale Aufregung (heise.de: „*Keine Strafen: Österreich zieht neuem Datenschutz die Zähne*") löste der „in letzter Sekunde" vor dem 25. Mai 2018 eingeführte § 11 DSG mit der Überschrift „*Verwarnung durch die Datenschutzbehörde*" aus, wonach insbesondere bei erstmaligen Verstößen die Datenschutzbehörde im Einklang mit Art. 58 DSGVO von ihren Abhilfebefugnissen insbesondere durch Verwarnen Gebrauch machen wird. Entgegen der irreführenden medialen Berichterstattung schließt dies nicht aus, dass auch bei erstmaligen Verstößen eine Bestrafung erfolgt (was durch die DSB auch inzwischen im Zusammenhang mit unzulässiger Videoüberwachung mehrmals erfolgt ist). Datenschutz-Compliance bleibt daher wichtig. (ii) Auch nach neuer Rechtslage können Datenträger und Programme sowie Bildübertragungs- und Bildaufzeichnungsgeräte für verfallen erklärt werden, (allerdings nur) wenn sie mit Verwaltungsübertretungen in Zusammenhang stehen. Daher gilt die Pflicht der Nachvollziehbarkeit der Behördenentscheidung (auch) hinsichtlich des Verfallsausspruchs weiterhin.

3.22. Oberster Gerichtshof (OGH) – zur Löschverpflichtungen der Staatsanwaltschaft nach StPO und nicht nach anderen Grundlagen (OGH 11Os69/18h am 02.04.2019 [Link]):

Die Staatsanwaltschaft ***** führte zur AZ 6 St 60/15t ein Ermittlungsverfahren gegen ***** und weitere Beschuldigte wegen des Vergehens des geheimen Nachrichtendienstes zum Nachteil Österreichs nach § 256 dritter Fall StGB sowie anderer strafbarer Handlungen, welches seit 4. April 2017 zur Gänze eingestellt ist.

Während des Ermittlungsverfahrens waren von einer unbekannten Person, angeblich von einem ehemaligen Mitarbeiter, aus der ***** GmbH stammende Daten auf Datenträgern gespeichert und diese unaufgefordert der Staatsanwaltschaft, den Sicherheitsbehörden, dem Bundesministerium für Justiz (nunmehr Bundesministerium für Verfassung, Reformen,

Deregulierung und Justiz) und anderen übermittelt worden.

Mit Schriftsätzen vom 5. Juli 2017 bzw vom 4. August 2017 beantragten sowohl ***** als auch die ***** GmbH bei der Staatsanwaltschaft ***** die Löschung sämtlicher personenbezogener Daten auf beim Akt befindlichen Datenträgern gemäß § 27 DSG 2000 iVm §§ 74, 75 StPO, weil die darauf enthaltenen Informationen aus der *****kanzlei der Antragsteller stammten, der ***** Verschwiegenheitspflicht unterlägen und – aus Sicht der Antragsteller – unter Verletzung strafprozessualer Vorschriften ermittelt worden seien, weshalb die Verwendung der Daten überhaupt, aber jedenfalls seit der Einstellung des Ermittlungsverfahrens unzulässig sei.

Die Staatsanwaltschaft verweigerte die Datenlöschung unter Hinweis auf (rechtskräftige) Entscheidungen des Oberlandesgerichts ***** mit der Begründung, dass danach weder die in Rede stehenden Datenträger in Umgehung des § 144 Abs 2 StPO rechtswidrig beschafft worden seien noch eine Verpflichtung zu deren Herausgabe oder zur Löschung der darauf gespeicherten Daten bestehe.

Das GOG umfasst keine eigenen Datenschutzansprüche, sondern regelt nur die Durchsetzung der nach dem DSG 2000 bestehenden – grundsätzlich auch für juristische Personen anerkannten (§ 4 Z 3 DSG 2000) – Datenschutzrechte bei Akten der Gerichtsbarkeit, sofern die in den Verfahrensgesetzen vorgesehenen Rechtsmittel kein Aufgreifen ermöglichen. Die Vorschriften der GOG in der geltenden Fassung dienen solcherart nicht dazu, in jenen Bereichen, in denen die Verfahrensgesetze die Verwendung von Daten (abschließend) regeln, das gerichtliche (Haupt-)Verfahren zu beeinflussen, zu korrigieren oder nachträglich zu kontrollieren. Eine den Verfahrensgesetzen entsprechende Verwendung von Daten ist daher auch aus datenschutzrechtlicher Sicht zulässig.

Eine Verpflichtung, Daten unverzüglich zu löschen, statuiert § 75 Abs 1 StPO – im Einklang mit § 27 Abs 1 DSG 2000 – für unrichtige oder entgegen den gesetzlichen Bestimmungen ermittelte Daten. Richtige und rechtmäßig ermittelte personenbezogene Daten sind (spätestens – zur verfassungs¬konformen Interpretation dieser Regelung im Sinn einer Maximalfrist vgl das Erkenntnis des VfGH vom 29. Juni 2012, G 7/12) nach sechzig Jahren im direkten Zugriff zu löschen (§ 75 Abs 3 StPO).

Die Strafprozessordnung normiert demnach einen (subjektiven) Anspruch (ua) auf Löschung von durch Staatsanwaltschaft und Gericht im Rahmen ihrer Aufgaben im Strafverfahren (§ 1 StPO) erlangten personenbezogenen Daten (§§ 74, 75 StPO). Berechtigten Löschungsanträgen einer betroffenen Person hat das zuständige Organ der Gerichtsbarkeit (je nach Verfahrensstadium also die Staatsanwaltschaft oder das Gericht) unverzüglich zu entsprechen. Eine abschlägige Entscheidung des Gerichts über einen solchen Antrag hat mit bekämpfbarem Beschluss zu ergehen (vgl §§ 35 Abs 2, 86, 87 StPO). Im Zuständigkeitsbereich der Staatsanwaltschaft (§ 20 StPO) wiederum steht jeder Person ein Einspruch an das Gericht zu, die ua behauptet, im Ermittlungsverfahren in einem subjektiven Recht verletzt zu sein, weil ihr die Staatsanwaltschaft die Ausübung eines in der Strafprozessordnung eingeräumten Rechtes (etwa jenem nach § 75 StPO) verweigert (§§ 106, 107 StPO). Der Oberste Gerichtshof hat bereits klargestellt, dass ein solcher Einspruch wegen Rechtsverletzung selbst gegen eine erst nach Einstellung des Ermittlungsverfahrens getroffene Entscheidung der Staatsanwaltschaft betreffend subjektive Rechte erhoben

werden kann. Die darüber ergangene gerichtliche Entscheidung kann (ua) der Einspruchswerber mit Beschwerde bekämpfen (§ 107 Abs 3 erster Satz StPO).

Ein auf die (unverzügliche) Löschung von in einem Strafverfahren verarbeiteten personenbezogenen Daten bezogener Anspruch ist, weil er nach dem oben Gesagten mit in der StPO eingeräumten Rechtsmitteln aufgegriffen werden kann, nicht Gegenstand des bloß subsidiären Verfahrens nach dem GOG.

4. EuGH Spruchpraxis

4.1. Urteil des Gerichtshofs (Große Kammer) am 10.07.2018 in der Rechtssache C-25/17 – Gemeinsame Verantwortlichkeit bei Zeugen Jehovas [Link]:

Die Erhebung personenbezogener Daten, die durch Mitglieder einer Religionsgemeinschaft im Rahmen einer Verkündigungstätigkeit von Tür zu Tür erfolgt, und die anschließenden Verarbeitungen dieser Daten unterfallen der Datenschutz-RL und sind von den Ausnahmen gemäß Art. 3 Abs. 2 dieser Richtlinie erfasst.

Eine Religionsgemeinschaft ist gemeinsam mit ihren als Verkündiger tätigen Mitgliedern als Verantwortliche für die Verarbeitungen personenbezogener Daten anzusehen, die durch diese Mitglieder im Rahmen einer Verkündigungstätigkeit von Tür zu Tür erfolgen, die von dieser Gemeinschaft organisiert und koordiniert wird und zu der sie ermuntert, ohne dass es hierfür erforderlich wäre, dass die Gemeinschaft Zugriff auf diese Daten hat oder ihren Mitgliedern nachweislich schriftliche Anleitungen oder Anweisungen zu diesen Datenverarbeitungen gegeben hat.

4.2. Urteil des Gerichtshofs (Große Kammer) am 05.06.2018 – In der Rechtssache C-210/16 - Facebook-Fanpage bzw Facebook-Insight [Link]

Die Wirtschaftsakademie Schleswig-Holstein bietet Bildungsdienstleistungen über eine auf Facebook unterhaltene Fanpage an. Fanpages sind Benutzerkonten, die bei Facebook von Privatpersonen oder Unternehmen eingerichtet werden können. Der Fanpage-Anbieter kann nach einer Registrierung bei Facebook die von diesem unterhaltene Plattform dazu benutzen, sich den Nutzern dieses sozialen Netzwerks sowie Personen, die die Fanpage besuchen, zu präsentieren und Äußerungen aller Art in den Medien- und Meinungsmarkt einzubringen. Die Betreiber von Fanpages können mit Hilfe der Funktion Facebook Insight, die ihnen Facebook als nicht abdingbaren Teil des Benutzungsverhältnisses kostenfrei zur Verfügung stellt, anonymisierte statistische Daten betreffend die Nutzer dieser Seiten erhalten. Diese Daten werden mit Hilfe sogenannter Cookies gesammelt, die jeweils einen eindeutigen Benutzercode enthalten, der für zwei Jahre aktiv ist und den Facebook auf der Festplatte des Computers oder einem anderen Datenträger der Besucher der Fanpage speichert. Der Benutzercode, der mit den Anmeldungsdaten solcher Nutzer, die bei Facebook registriert sind, verknüpft werden kann, wird beim Aufrufen der Fanpages erhoben und verarbeitet. Insoweit geht aus der Vorlageentscheidung hervor, dass – jedenfalls in dem für das Ausgangsverfahren relevanten Zeitraum – weder die Wirtschaftsakademie noch die Facebook Ireland Ltd auf die Tatsache der Speicherung und die Funktionsweise dieses Cookies oder die nachfolgende Datenverarbeitung hingewiesen haben.

Es ist festzustellen, dass im vorliegenden Fall in erster Linie die Facebook Inc. und, was die

Union betrifft, Facebook Ireland über die Zwecke und Mittel der Verarbeitung der personenbezogenen Daten der Facebook-Nutzer und der Personen entscheiden, die die auf Facebook unterhaltenen Fanpages besucht haben, und somit unter den Begriff des „für die Verarbeitung Verantwortlichen“ fallen, was in der vorliegenden Rechtssache nicht in Zweifel gezogen wird.

Jede Person, die eine Fanpage auf Facebook einrichten möchte, mit Facebook Ireland einen speziellen Vertrag über die Eröffnung einer solchen Seite schließt und unterzeichnet dazu die Nutzungsbedingungen dieser Seite einschließlich der entsprechenden Cookie-Richtlinie.

Auch wenn der bloße Umstand der Nutzung eines sozialen Netzwerks wie Facebook für sich genommen einen Facebook-Nutzer nicht für die von diesem Netzwerk vorgenommene Verarbeitung personenbezogener Daten mitverantwortlich macht, ist indes darauf hinzuweisen, dass der Betreiber einer auf Facebook unterhaltenen Fanpage mit der Einrichtung einer solchen Seite Facebook die Möglichkeit gibt, auf dem Computer oder jedem anderen Gerät der Person, die seine Fanpage besucht hat, Cookies zu platzieren, unabhängig davon, ob diese Person über ein Facebook-Konto verfügt.

In diesem Rahmen geht aus den dem Gerichtshof unterbreiteten Angaben hervor, dass die Einrichtung einer Fanpage auf Facebook von Seiten ihres Betreibers eine Parametrierung u. a. entsprechend seinem Zielpublikum sowie den Zielen der Steuerung oder Förderung seiner Tätigkeiten impliziert, die sich auf die Verarbeitung personenbezogener Daten zum Zweck der Erstellung der aufgrund der Besuche der Fanpage erstellten Statistiken auswirkt. Mit Hilfe von durch Facebook zur Verfügung gestellten Filtern kann der Betreiber die Kriterien festlegen, nach denen diese Statistiken erstellt werden sollen, und sogar die Kategorien von Personen bezeichnen, deren personenbezogene Daten von Facebook ausgewertet werden. Folglich trägt der Betreiber einer auf Facebook unterhaltenen Fanpage zur Verarbeitung der personenbezogenen Daten der Besucher seiner Seite bei.

Insbesondere kann der Fanpage-Betreiber demografische Daten über seine Zielgruppe – und damit die Verarbeitung dieser Daten – verlangen, so u. a. Tendenzen in den Bereichen Alter, Geschlecht, Beziehungsstatus und berufliche Situation, Informationen über den Lebensstil und die Interessen seiner Zielgruppe und Informationen über die Käufe und das Online-Kaufverhalten der Besucher seiner Seite, die Kategorien von Waren oder Dienstleistungen, die sie am meisten interessieren, sowie geografische Daten, die ihn darüber informieren, wo spezielle Werbeaktionen durchzuführen oder Veranstaltungen zu organisieren sind, und ihm ganz allgemein ermöglichen, sein Informationsangebot so zielgerichtet wie möglich zu gestalten.

Zwar werden die von Facebook erstellten Besucherstatistiken ausschließlich in anonymisierter Form an den Betreiber der Fanpage übermittelt, jedoch beruht die Erstellung dieser Statistiken auf der vorhergehenden Erhebung – durch die von Facebook auf dem Computer oder jedem anderen Gerät der Personen, die diese Seite besucht haben, gesetzten Cookies – und der Verarbeitung der personenbezogenen Daten dieser Besucher für diese statistischen Zwecke.

Unter diesen Umständen ist festzustellen, dass der Betreiber einer auf Facebook unterhaltenen Fanpage wie die Wirtschaftsakademie durch die von ihm vorgenommene

Parametrierung u. a. entsprechend seinem Zielpublikum sowie den Zielen der Steuerung oder Förderung seiner Tätigkeiten an der Entscheidung über die Zwecke und Mittel der Verarbeitung der personenbezogenen Daten der Besucher seiner Fanpage beteiligt ist. Daher ist der Betreiber im vorliegenden Fall als in der Union gemeinsam mit Facebook Ireland für diese Verarbeitung Verantwortlicher einzustufen.

Der Umstand, dass ein Betreiber einer Fanpage die von Facebook eingerichtete Plattform nutzt, um die dazugehörigen Dienstleistungen in Anspruch zu nehmen, kann diesen nämlich nicht von der Beachtung seiner Verpflichtungen im Bereich des Schutzes personenbezogener Daten befreien.

Im Übrigen ist hervorzuheben, dass die bei Facebook unterhaltenen Fanpages auch von Personen besucht werden können, die keine Facebook-Nutzer sind und somit nicht über ein Benutzerkonto bei diesem sozialen Netzwerk verfügen. In diesem Fall erscheint die Verantwortlichkeit des Betreibers der Fanpage hinsichtlich der Verarbeitung der personenbezogenen Daten dieser Personen noch höher, da das bloße Aufrufen der Fanpage durch Besucher automatisch die Verarbeitung ihrer personenbezogenen Daten auslöst.

Unter diesen Umständen trägt die Anerkennung einer gemeinsamen Verantwortlichkeit des Betreibers des sozialen Netzwerks und des Betreibers einer bei diesem Netzwerk unterhaltenen Fanpage im Zusammenhang mit der Verarbeitung personenbezogener Daten der Besucher dieser Fanpage dazu bei, einen umfassenderen Schutz der Rechte sicherzustellen, über die die Personen verfügen, die eine Fanpage besuchen.

Klarzustellen ist, dass das Bestehen einer gemeinsamen Verantwortlichkeit, aber nicht zwangsläufig eine gleichwertige Verantwortlichkeit der verschiedenen Akteure zur Folge hat, die von einer Verarbeitung personenbezogener Daten betroffen sind. Vielmehr können diese Akteure in die Verarbeitung personenbezogener Daten in verschiedenen Phasen und in unterschiedlichem Ausmaß in der Weise einbezogen sein, dass der Grad der Verantwortlichkeit eines jeden von ihnen unter Berücksichtigung aller maßgeblichen Umstände des Einzelfalls zu beurteilen ist.

4.3. Urteil des Gerichtshofs (Große Kammer) am 29.07.2019 – In der Rechtssache C-40/17 – Fashion ID bzw. gemeinsame Verantwortlichkeit für personenbezogenes Facebook-Retargeting / Facebook-Tracking / Facebook Cookies [Link])

Im vorliegenden Fall ergibt sich für den EuGH, allerdings vorbehaltlich der Nachprüfung durch das vorlegende Gericht, aus den dem Gerichtshof vorliegenden Akten, dass Fashion ID es dadurch, dass sie den „Gefällt mir“-Button von Facebook Ireland in ihre Website eingebunden hat, offenbar ermöglicht hat, personenbezogene Daten der Besucher ihrer Website zu erhalten. Diese Möglichkeit entsteht ab dem Zeitpunkt des Aufrufens einer solchen Seite, und zwar unabhängig davon, ob diese Besucher Mitglieder des sozialen Netzwerks Facebook sind, ob sie den „Gefällt mir“-Button von Facebook angeklickt haben oder auch ob sie von diesem Vorgang Kenntnis haben.

Unter Berücksichtigung dieser Informationen ist festzustellen, dass die Vorgänge der Verarbeitung personenbezogener Daten, für die Fashion ID gemeinsam mit Facebook Ireland über die Zwecke und Mittel entscheiden kann, im Rahmen der Definition des Begriffs

„Verarbeitung personenbezogener Daten“ in Art. 2 Buchst. b der Richtlinie 95/46 das Erheben der personenbezogenen Daten der Besucher ihrer Website und deren Weitergabe durch Übermittlung sind. Dagegen ist nach diesen Informationen auf den ersten Blick ausgeschlossen, dass Fashion ID über die Zwecke und Mittel der Vorgänge der Verarbeitung personenbezogener Daten entscheidet, die Facebook Ireland nach der Übermittlung dieser Daten an sie vorgenommen hat, so dass Fashion ID für diese Vorgänge nicht als verantwortlich im Sinne von Art. 2 Buchst. d angesehen werden kann.

Mit der Einbindung eines solchen Social Plugins in ihre Website hat Fashion ID im Übrigen entscheidend das Erheben und die Übermittlung von personenbezogenen Daten der Besucher dieser Seite zugunsten des Anbieters dieses Plugins, im vorliegenden Fall Facebook Ireland, beeinflusst, die ohne Einbindung dieses Plugins nicht erfolgen würden.

Unter diesen Umständen und vorbehaltlich der insoweit vom vorlegenden Gericht vorzunehmenden Nachprüfungen ist davon auszugehen, dass Facebook Ireland und Fashion ID über die Mittel, die dem Erheben personenbezogener Daten der Besucher der Website von Fashion ID und deren Weitergabe durch Übermittlung zugrunde lagen, gemeinsam entschieden haben.

Was die Zwecke dieser Vorgänge der Verarbeitung personenbezogener Daten betrifft, scheint es, dass die Einbindung des „Gefällt mir“-Buttons von Facebook durch Fashion ID in ihre Website ihr ermöglicht, die Werbung für ihre Produkte zu optimieren, indem diese im sozialen Netzwerk Facebook sichtbarer gemacht werden, wenn ein Besucher ihrer Website den Button anklickt. Um in den Genuss dieses wirtschaftlichen Vorteils kommen zu können, der in einer solchen verbesserten Werbung für ihre Produkte besteht, scheint Fashion ID mit der Einbindung eines solchen Buttons in ihre Website zumindest stillschweigend in das Erheben personenbezogener Daten der Besucher ihrer Website und deren Weitergabe durch Übermittlung eingewilligt zu haben. Dabei werden diese Verarbeitungsvorgänge im wirtschaftlichen Interesse sowohl von Fashion ID als auch von Facebook Ireland durchgeführt, für die die Tatsache, über diese Daten für ihre eigenen wirtschaftlichen Zwecke verfügen zu können, die Gegenleistung für den Fashion ID gebotenen Vorteil darstellt.

Daher kann, vorbehaltlich der vom vorlegenden Gericht vorzunehmenden Nachprüfung, davon ausgegangen werden, dass Fashion ID und Facebook Ireland gemeinsam über die Zwecke der Vorgänge des Erhebens der im Ausgangsverfahren in Rede stehenden personenbezogenen Daten und der Weitergabe durch Übermittlung entscheiden.

Mit seiner vierten Frage möchte das vorlegende Gericht wissen, ob in einer Situation wie der im Ausgangsverfahren in Rede stehenden, in der der Betreiber einer Website in diese Website ein Social Plugin einbindet, das den Browser des Besuchers dieser Website veranlasst, Inhalte des Anbieters dieses Plugins anzufordern und hierzu personenbezogene Daten an diesen Anbieter zu übermitteln, bei der Anwendung von Art. 7 Buchst. f der Richtlinie 95/46 auf das berechtigte Interesse dieses Betreibers oder das berechtigte Interesse des genannten Anbieters abzustellen ist.

Vorab ist darauf hinzuweisen, dass diese Frage nach Ansicht der Kommission für die Entscheidung des Ausgangsrechtsstreits unerheblich ist, da die von Art. 5 Abs. 3 der Richtlinie 2002/58 verlangte Einwilligung der betroffenen Personen nicht eingeholt wurde.

Nach Art. 7 Buchst. f der Richtlinie 95/46, um dessen Auslegung das vorlegende Gericht ersucht, ist die Verarbeitung personenbezogener Daten zulässig, wenn sie zur Verwirklichung des berechtigten Interesses erforderlich ist, das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, denen die Daten übermittelt werden, sofern nicht das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person, die gemäß Art. 1 Abs. 1 der Richtlinie 95/46 geschützt sind, überwiegen. Art. 7 Buchst. f enthält somit für die Zulässigkeit der Verarbeitung personenbezogener Daten drei kumulative Voraussetzungen: 1. berechtigtes Interesse, das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, denen die Daten übermittelt werden, 2. Erforderlichkeit der Verarbeitung der personenbezogenen Daten zur Verwirklichung des berechtigten Interesses und 3. kein Überwiegen der Grundrechte und Grundfreiheiten der betroffenen Person (Urteil vom 4. Mai 2017, Rīgas satiksme, C‑13/16, EU:C:2017:336, Rn. 28).

Da angesichts der Antwort auf die zweite Frage in einer Situation wie der im Ausgangsverfahren in Rede stehenden der Betreiber einer Website, der in diese Website ein Social Plugin einbindet, das den Browser des Besuchers dieser Website veranlasst, Inhalte des Anbieters dieses Plugins anzufordern und hierzu personenbezogene Daten des Besuchers an diesen Anbieter zu übermitteln, gemeinsam mit diesem Anbieter als für die Vorgänge der Verarbeitung – d. h. das Erheben und die Weitergabe durch Übermittlung – von personenbezogenen Daten der Besucher seiner Website Verantwortlicher angesehen werden kann, ist es erforderlich, dass jeder dieser Verantwortlichen mit diesen Verarbeitungsvorgängen ein berechtigtes Interesse im Sinne von Art. 7 Buchst. f der Richtlinie 95/46 wahrnimmt, damit diese Vorgänge für jeden Einzelnen von ihnen gerechtfertigt sind.

Demnach ist auf die vierte Frage zu antworten, dass es in einer Situation wie der im Ausgangsverfahren in Rede stehenden, in der der Betreiber einer Website in diese Website ein Social Plugin einbindet, das den Browser des Besuchers dieser Website veranlasst, Inhalte des Anbieters dieses Plugins anzufordern und hierzu personenbezogene Daten des Besuchers an diesen Anbieter zu übermitteln, erforderlich ist, dass der Betreiber und der Anbieter mit diesen Verarbeitungsvorgängen jeweils ein berechtigtes Interesse im Sinne von Art. 7 Buchst. f der Richtlinie 95/46 wahrnehmen, damit diese Vorgänge für jeden Einzelnen von ihnen gerechtfertigt sind.

Wie sich aus der Antwort auf die zweite Frage ergibt, kann der Betreiber einer Website, der in diese Website ein Social Plugin einbindet, das den Browser des Besuchers dieser Website veranlasst, Inhalte des Anbieters dieses Plugins anzufordern und hierzu personenbezogene Daten dieses Besuchers an diesen Anbieter zu übermitteln, als für die Verarbeitung Verantwortlicher im Sinne von Art. 2 Buchst. d der Richtlinie 95/46 angesehen werden. Dabei ist diese Verantwortlichkeit jedoch auf den Vorgang oder die Vorgänge der Datenverarbeitung beschränkt, für den bzw. für die er tatsächlich über die Zwecke und Mittel entscheidet.

Daher müssen die Verpflichtungen, die nach der Richtlinie 95/46 diesem für die Verarbeitung Verantwortlichen obliegen, wie etwa die Verpflichtung, die Einwilligung der betroffenen

Person gemäß Art. 2 Buchst. h und Art. 7 Buchst. a dieser Richtlinie einzuholen, sowie die Informationspflicht nach Art. 10 der Richtlinie den Vorgang oder die Vorgänge der Verarbeitung personenbezogener Daten betreffen, für den bzw. für die er tatsächlich über die Zwecke und Mittel entscheidet.

Wenn im vorliegenden Fall der Betreiber einer Website, der in diese Website ein Social Plugin einbindet, das den Browser des Besuchers dieser Website veranlasst, Inhalte des Anbieters dieses Plugins anzufordern und hierzu personenbezogene Daten des Besuchers an diesen Anbieter zu übermitteln, gemeinsam mit diesem Anbieter als für die Vorgänge des Erhebens personenbezogener Daten dieses Besuchers und deren Weitergabe durch Übermittlung verantwortlich angesehen werden kann, betrifft seine Verpflichtung, die Einwilligung der betroffenen Person gemäß Art. 2 Buchst. h und Art. 7 Buchst. a dieser Richtlinie einzuholen, sowie seine Informationspflicht nach Art. 10 der Richtlinie nur diese Vorgänge. Dagegen erstrecken sich diese Verpflichtungen nicht auf Vorgänge der Verarbeitung personenbezogener Daten, die andere, diesen Vorgängen vor- oder nachgelagerte Phasen betreffen, die die Verarbeitung der in Rede stehenden personenbezogenen Daten gegebenenfalls mit sich bringt.

Was die Einwilligung nach Art. 2 Buchst. h und Art. 7 Buchst. a der Richtlinie 95/46 betrifft, so muss diese vor dem Erheben der Daten der betroffenen Person und deren Weitergabe durch Übermittlung erklärt werden. Daher obliegt es dem Betreiber der Website und nicht dem Anbieter des Social Plugins, diese Einwilligung einzuholen, da der Verarbeitungsprozess der personenbezogenen Daten dadurch ausgelöst wird, dass ein Besucher diese Website aufruft. Wie der Generalanwalt in Nr. 132 seiner Schlussanträge ausgeführt hat, entspräche es nämlich nicht einer wirksamen und rechtzeitigen Wahrung der Rechte der betroffenen Person, wenn die Einwilligung lediglich gegenüber dem gemeinsam für die Verarbeitung Verantwortlichen erklärt würde, der erst zu einem späteren Zeitpunkt beteiligt ist, also gegenüber dem Anbieter dieses Plugins. Die Einwilligung, die dem Betreiber gegenüber zu erklären ist, betrifft jedoch nur den Vorgang oder die Vorgänge der Verarbeitung personenbezogener Daten, für den bzw. für die er tatsächlich über die Zwecke und Mittel entscheidet.

Das Gleiche gilt für die Informationspflicht nach Art. 10 der Richtlinie 95/46.