

D155.027, 2021-0.586.257

[Anmerkung Bearbeiter: Namen und Firmen, Rechtsformen und Produktbezeichnungen, Adressen (inkl. URLs, IP- und E-Mail-Adressen), Aktenzahlen (und dergleichen), etc., sowie deren Initialen und Abkürzungen können aus Pseudonymisierungsgründen abgekürzt und/oder verändert sein.]

T E I L B E S C H E I D

S P R U C H

Die Datenschutzbehörde entscheidet über die Datenschutzbeschwerde von Kai Mustermann (Beschwerdeführer) vom 18. August 2020, vertreten durch NOYB - Europäisches Zentrum für digitale Rechte, Goldschlagstraße 172/4/3/2, 1140 Wien, ZVR: 1354838270, gegen 1) Selina Musterfrau GmbH (vormals: Jens Mustermann GmbH) (Erstbeschwerdegegnerin), vertreten durch XY und 2) Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA (Zweitbeschwerdegegner), vertreten durch YZ, wegen einer Verletzung der allgemeinen Grundsätze der Datenübermittlung gemäß Art. 44 DSGVO wie folgt:

1. Der Bescheid der Datenschutzbehörde vom 2. Oktober 2020, Zl. D155.027, 2020-0.527.385, wird behoben.
2. Der Beschwerde gegen die Erstbeschwerdegegnerin wird stattgegeben und es wird festgestellt, dass
 - a) die Erstbeschwerdegegnerin als Verantwortliche durch Implementierung des Tools „Google Analytics“ auf ihrer Website unter www.xyz.at zumindest am 14. August 2020 personenbezogene Daten des Beschwerdeführers (dies sind zumindest einzigartige Nutzer-Identifikations-Nummern, IP-Adresse und Browserparameter) an den Zweitbeschwerdegegner übermittelt hat,
 - b) die Standarddatenschutzklauseln, die die Erstbeschwerdegegnerin mit dem Zweitbeschwerdegegner abgeschlossen hat, kein angemessenes Schutzniveau gemäß Art. 44 DSGVO bieten, da
 - i) der Zweitbeschwerdegegner als Anbieter elektronischer Kommunikationsdienste im Sinne von 50 U.S. Code § 1881(b)(4) zu

qualifizieren ist und als solcher der Überwachung durch US-Geheimdienste gemäß 50 U.S. Code § 1881a („FISA 702“) unterliegt, und

- ii) die Maßnahmen, die zusätzlich zu den in Spruchpunkt 2. b) genannten Standarddatenschutzklauseln getroffen wurden, nicht effektiv sind, da diese die Überwachungs- und Zugriffsmöglichkeiten durch US-Nachrichtendienste nicht beseitigen,
 - c) im vorliegenden Fall kein anderes Instrument gemäß Kapitel V der DSGVO für die in Spruchpunkt 2.a) angeführte Datenübermittlung herangezogen werden kann und die Erstbeschwerdegegnerin deshalb für die im Rahmen der in Spruchpunkt 2.a) angeführte Datenübermittlung kein angemessenes Schutzniveau gemäß Art. 44 DSGVO gewährleistet hat.
3. Die Beschwerde gegen den Zweitbeschwerdegegner wegen einer Verletzung der allgemeinen Grundsätze der Datenübermittlung gemäß Art. 44 DSGVO wird abgewiesen.

Rechtsgrundlagen: Art. 4 Z 1, Z 2, Z 7 und 8, Art. 5, Art. 44, Art. 46 Abs. 1 und Abs. 2 lit. c, Art. 51 Abs. 1, Art. 57 Abs. 1 lit. d und lit. f, Art. 77 Abs. 1, Art. 80 Abs. 1 sowie Art. 93 Abs. 2 der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung, DSGVO), ABl. Nr. L 119 vom 4.5.2016 S. 1; §§ 18 Abs. 1 sowie 24 Abs. 1, Abs. 2 Z 5 und Abs. 5 des Datenschutzgesetzes (DSG), BGBl. I Nr. 165/1999 idgF; § 68 Abs. 2 des Allgemeinen Verwaltungsverfahrensgesetzes 1991 (AVG), BGBl. 51/1991 idgF.

B E G R Ü N D U N G

A. Vorbringen der Parteien und Verfahrensgang

A.1. Der Beschwerdeführer brachte in seiner Eingabe vom 18. August 2020 zusammengefasst Folgendes vor:

Er habe am 14. August 2020, um 10:45 Uhr, die Website der Erstbeschwerdegegnerin unter www.xyz.at besucht. Während des Besuchs sei er in seinem Google-Konto eingeloggt gewesen, welche mit der E-Mail-Adresse des Beschwerdeführers, musteremail123@gmail.com, verknüpft sei. Die Erstbeschwerdegegnerin habe auf ihrer Website einen HTML-Code für Google-Dienste (inklusive Google Analytics) eingebettet. Im Verlauf des Besuchs habe die Erstbeschwerdegegnerin personenbezogene Daten, nämlich zumindest die IP-Adresse und die Cookie-Daten des Beschwerdeführers verarbeitet. Dabei seien einige dieser Daten an den Zweitbeschwerdegegner übermittelt worden. Eine solche Datenübermittlung erfordere eine Rechtsgrundlage gemäß den Art. 44 ff DSGVO.

Nach dem Urteil des EuGH vom 16. Juli 2020, Rs C-11/18 („Schrems II“), könnten sich die Beschwerdegegner für eine Datenübermittlung in die USA nicht mehr auf eine Angemessenheitsentscheidung („Privacy Shield“) nach Art. 45 DSGVO stützen. Die Erstbeschwerdegegnerin dürfe die Datenübermittlung auch nicht auf Standarddatenschutzklauseln stützen, wenn das Bestimmungsdrittland nach Maßgabe des Unionsrechts keinen angemessenen Schutz der auf der Grundlage von Standarddatenschutzklauseln übermittelten personenbezogenen Daten gewährleiste. Der Zweitbeschwerdegegner sei als Anbieter elektronischer Kommunikationsdienste im Sinne von 50 U.S.Code § 1881(b)(4) zu qualifizieren und unterliege als solcher der Überwachung durch US-Geheimdienste gemäß 50 U.S.Code § 1881a („FISA 702“). Der Zweitbeschwerdegegner stelle der US-Regierung gemäß 50 U.S. Code § 1881a aktiv personenbezogene Daten zur Verfügung.

Folglich seien die Beschwerdegegner nicht in der Lage, einen angemessenen Schutz der personenbezogenen Daten des Beschwerdeführers zu gewährleisten, wenn dessen Daten an den Zweitbeschwerdegegner übermittelt werden. Die Übermittlung der Daten des Beschwerdeführers in die USA sei unrechtmäßig. Der Beschwerde waren mehrere Beilagen beigelegt.

A.2. Mit Stellungnahme vom 16. Dezember 2020 brachte die Erstbeschwerdegegnerin zusammengefasst Folgendes vor:

Die Erstbeschwerdegegnerin sei nur in Österreich ansässig. Sie sei für die Entscheidung verantwortlich, das Tool auf der Webseite www.xyz.at einzubetten. Das Tool werde eingesetzt, um allgemeine statistische Auswertungen über das Verhalten der Website-Besucher zu ermöglichen. Das Tool erlaube allerdings nicht, den Content an einen konkreten Websiteuser anzupassen, da die

Auswertung anonym durchgeführt werde und kein Bezug zu einem bestimmten User ermöglicht werde. Auch Nutzer-IP-Adressen würden vor Speicherung oder Übermittlung anonymisiert werden („IP-Anonymisierung“). Der sogenannte User Agent String diene dazu, dem Server mitzuteilen, mit welcher Systemspezifikation der User auf den Server zugreife. Dabei würden ohne Personenbezug nur Gerät, Betriebssystem- und -version, Browser- und Browserversion und der Gerätetyp angezeigt werden. Im besten Fall sei eine Zuordnung zu einem bestimmten Gerät, niemals jedoch zu einer konkreten Person, die das Gerät nutze, möglich. Die Verarbeitung der anonymen Statistiken erfolge überwiegend in Rechenzentren in Europa, allerdings auch durch den Zweitbeschwerdegegner auf Servern außerhalb des EWR.

Sofern die DSGVO anwendbar sei, sei die Erstbeschwerdegegnerin Verantwortliche und der Zweitbeschwerdegegner sei Auftragsverarbeiter. Es sei eine Auftragsverarbeitervereinbarung abgeschlossen worden. Da keine personenbezogenen Daten übermittelt werden würden, sei das Urteil des EuGH vom 16. Juli 2020 in der Rechtssache C311/18 nicht anwendbar. Um jedoch für eine etwaige Überlassung von personenbezogenen Daten an den Zweitbeschwerdegegner Vorkehrungen zu treffen – zB. den Fall, dass die IP-Anonymisierung aufgrund eines Data Breaches deaktiviert werde –, habe der Erstbeschwerdegegner mit dem Zweitbeschwerdegegner eine Auftragsverarbeitervereinbarung abgeschlossen, als auch Standarddatenschutzklauseln (SDK) einbezogen. Dies sei rein aus Vorsichtsgründen implementiert worden. Der Zweitbeschwerdegegner habe weitere technische und organisatorische Maßnahmen gesetzt, um ein hohes Datenschutzniveau für die über die Tools verarbeiteten Daten zu bieten. Der Stellungnahme waren mehrere Beilagen beigelegt.

A.3. Mit Stellungnahme vom 22. Jänner 2021 brachte der Beschwerdeführer zusammengefasst Folgendes vor:

Bei einem Auftragsverarbeiter in einem Drittland sei ein Bruch der Anonymisierung nicht durchsetzbar oder feststellbar. Im Zweifel gelte 50 U.S.C § 1881a und nicht ein Werbetext auf der Google-Website. Die zuerst verarbeiteten personenbezogenen Daten würden erst nachträglich in einem zweiten Schritt anonymisiert werden. Diese nach Übertragung möglicherweise erfolgte Anonymisierung wirke sich nicht auf die vorherige Verarbeitung aus. Die Stellungnahme enthält an dieser Stelle eine nähere technische Beschreibung.

Abgesehen davon berufe sich der Beschwerdeführer nicht nur auf die Verarbeitung seiner IP-Adresse, sondern auch anderer personenbezogener Daten, etwa Cookie-Daten. Zum Zeitpunkt des Website-Besuchs sei er in sein privates Google-Konto eingeloggt gewesen. Es seien „Google“-Cookies gesetzt worden. Um eine Verletzung der Art. 44 ff DSGVO zu verhindern, sei eine gänzliche Entfernung des Tools nötig und ein Wechsel zu einem anderen Tool ohne Datenübermittlung in die USA zu empfehlen. Sofern die Erstbeschwerdegegnerin der Überzeugung sei, dass keine personenbezogenen Daten verarbeitet würden, sei der Abschluss von Auftragsverarbeitungsbedingungen widersinnig. Der Stellungnahme waren mehrere Beilagen beigelegt.

A.4. Mit Stellungnahme vom 9. April 2021 übermittelte der Zweitbeschwerdegegner seine Antworten zum Fragenkatalog der Datenschutzbehörde.

A.5. Mit Stellungnahme vom 4. Mai 2021 brachte die Erstbeschwerdegegnerin zur Stellungnahme des Zweitbeschwerdegegners vom 9. April 2021 zusammengefasst Folgendes vor:

Die Erstbeschwerdegegnerin verwende lediglich die kostenlose Version von Google Analytics. Dabei sei sowohl den Nutzungsbedingungen als auch den SDK zugestimmt worden. Dabei sei weder die Google Analytics 4 Version implementiert, noch die Datenfreigabe-Einstellung aktiviert worden. Der Code sei mit der Anonymisierungsfunktion eingebettet worden. Der Zweitbeschwerdegegner werde nur als Auftragsverarbeiter eingesetzt. Die Weisungen erteile die Erstbeschwerdegegnerin über die Einstellungen der Google-Analytics-Benutzeroberfläche und über das globale Website Tag. Google Signals werde nicht eingesetzt. Die Erstbeschwerdegegnerin verfüge über kein eigenes Authentifizierungssystem und benutze auch keine Benutzer-ID-Funktion. Aktuell stütze man sich nicht auf die Ausnahmeregelung des Art. 49 Abs. 1 DSGVO.

A.6. Mit Stellungnahme vom 5. Mai 2021 brachte der Beschwerdeführer zur Stellungnahme des Zweitbeschwerdegegners vom 9. April 2021 zusammengefasst Folgendes vor:

Die Beschwerde richte sich gegen den Erst- und Zweitbeschwerdegegner. Google Ireland Limited sei nicht Partei des Verfahrens. Die Datenschutzbehörde sei für den Zweitbeschwerdegegner unmittelbar zuständig, dieser habe gegen Art. 44 ff DSGVO verstoßen. Der Zweitbeschwerdegegner sei als Auftragsverarbeiter Normadressat von Kapitel V DSGVO. Der Zweitbeschwerdegegner stelle außer Streit, dass alle durch Google Analytics erhobenen Daten in den USA gehostet werden würden.

Zumindest einige der anlässlich des Websitebesuchs am 14. August 2020 gesetzten Cookies würden eindeutige Nutzer-Identifikations-Nummern enthalten. In der Transaktion zwischen dem Browser des Beschwerdeführers und <https://tracking.XYZ123.at>, die zum angeführten Datum gestartet worden sei, seien die Nutzer-Identifikations-Nummern „_gads“, „_ga“ und „_gid“ gesetzt worden. Diese Nummern seien in Folge an <https://www.google-analytics.com/> übermittelt worden. Es handle sich bei den Nummern um „Online-Kennungen“, die der Identifizierbarkeit natürlicher Personen dienen und einem Nutzer konkret zugeordnet werden würden. Im Hinblick auf die IP-Adresse sei festzuhalten, dass Kapitel V DSGVO keine Ausnahmen für „nachträglich anonymisierte Daten“ vorsehe. Es sei davon auszugehen, dass die IP-Adresse des Beschwerdeführers nicht einmal in allen Transaktionen anonymisiert worden sei. Der Antrag auf Verhängung einer Geldbuße werde zurückgezogen, dies sei nunmehr eine Anregung.

A.7. Mit Stellungnahme vom 10. Juni 2021 brachte der Zweitbeschwerdegegner zusammengefasst Folgendes vor:

Die Aktivlegitimation des Beschwerdeführers sei nicht festgestellt, da nicht nachgewiesen worden sei, dass es sich bei den übermittelten Daten um personenbezogene Daten des Beschwerdeführers handle. Es handle sich bei den fraglichen Cookies um First Party Cookies, die unter der Domain www.xyz.at gesetzt worden seien. Es handle sich daher um Cookies des Erst- und nicht des Zweitbeschwerdegegners. Demnach handle es sich nicht um einzigartige Google-Analytics-Cookie-IDs pro Nutzer, die auf mehreren Websites verwendet würden, die Google Analytics nutzten. Ein Nutzer habe unterschiedliche cid-Nummern für verschiedene Websites. Es sei nicht festgestellt, dass die gegenständlichen Nummern den Beschwerdeführer identifizierbar machen würden. Das Vorbringen enthält an dieser Stelle weitere technische Ausführungen zu den eingesetzten Cookies. Im Hinblick auf die IP-Adresse sei zu prüfen, ob die IP-Adresse des mit dem Internet verbundenen Geräts tatsächlich dem Beschwerdeführer zuzuordnen sei und ob der Verantwortliche oder „eine andere Person“ die rechtlichen Mittel habe, um Anschlussinhaberinformationen von dem betreffenden Anbieter zu erhalten.

Als Auftragsverarbeiter stelle der Zweitbeschwerdegegner dem Website-Betreiber zahlreiche Konfigurationsmöglichkeiten von Google Analytics zur Verfügung. Auf Grundlage der erhaltenen Informationen sei festzuhalten, dass die Erstbeschwerdegegnerin Google Analytics so konfiguriert habe, wie angegeben. Durch einen möglichen Konfigurationsfehler habe die Erstbeschwerdegegnerin die IP-Anonymisierungsfunktion nicht in allen Fällen aktiviert. Unter normalen Betriebsbedingungen und soweit Nutzer mit Sitz in der EU betroffen seien, befinde sich ein Webserver im EWR, weshalb die IP-Anonymisierung grundsätzlich innerhalb des EWR erfolge. Im vorliegenden Fall seien normale Betriebsbedingungen vorgelegen.

Am 14. August 2020 habe das Konto musteremail123@gmail.com die Web-&-App Aktivitäten Einstellung aktiviert. Allerdings habe sich das Konto nicht entschieden, Aktivitäten von Websites einzuschließen, die Google Dienste nutzen. Da die Erstbeschwerdegegnerin nach eigenen Angaben auch Google-Signals nicht aktiviert habe, sei der Zweitbeschwerdegegner demnach nicht in der Lage, festzustellen, dass der Nutzer des Kontos musteremail123@gmail.com diese Website besucht habe.

Im Hinblick auf den internationalen Datenverkehr sei festzuhalten, dass – selbst unter der Annahme, dass es sich um personenbezogene Daten des Beschwerdeführers handle – diese ihrer Art nach im Hinblick auf Quantität und Qualität begrenzt seien. Soweit die übermittelten Daten überhaupt als personenbezogene Daten zu qualifizieren seien, würde es sich auch um pseudonyme Daten handeln. Es seien Standardvertragsklauseln mit der Erstbeschwerdegegnerin abgeschlossen worden, zusätzlich seien ergänzende Maßnahmen implementiert worden. Der Zweitbeschwerdegegner lege keine Nutzerdaten gemäß EO 12333 offen. FISA § 702 sei im vorliegenden Fall angesichts der Verschlüsselung und der Anonymisierung von IP-Adressen irrelevant. Die Art. 44 ff DSGVO könnten nicht Gegenstand eines Beschwerdeverfahrens nach Art. 77 Abs. 1 DSGVO sein, weshalb die Beschwerde dahingehend zurückzuweisen sei. Die Art. 44 ff DSGVO seien im Hinblick auf den Zweitbeschwerdegegner als Datenimporteur auch nicht anwendbar.

A.8. Mit Stellungnahmen vom 18. und 24. Juni 2021 brachte die Erstbeschwerdegegnerin zusammengefasst Folgendes vor:

Im Rahmen eines Asset-Deals sei mit Wirkung Musterdatum Musterjahr die Website www.xyz.at auf die XYZ123 GmbH in XY übertragen worden. Im Anschluss sei die Erstbeschwerdegegnerin von xyz123.at GmbH in Neue Muster GmbH umbenannt worden. Darüber hinaus habe die Erstbeschwerdegegnerin den Zweitbeschwerdegegner angewiesen, alle über die Google-Analytics-Properties gesammelten Daten sofort zu löschen. Der Konfigurationsfehler im Zusammenhang mit der IP-Anonymisierungsfunktion sei behoben worden. In der Zwischenzeit habe der Zweitbeschwerdegegner die endgültige Löschung aller Daten bestätigt, als Nachweis werde eine Beilage vorgelegt. Es werde angeregt, das Verfahren gemäß § 24 Abs. 6 DSGVO einzustellen.

A.9. Mit Stellungnahmen vom 9. Juli 2021 brachte der Zweitbeschwerdegegner zusammengefasst Folgendes vor:

Eine Angemessenheitsbeurteilung sei nach Ansicht des Europäischen Datenschutzausschusses (EDSA) nicht auf die Prüfung der Rechtsvorschriften des Drittlandes beschränkt, sondern müsse auch alle spezifischen Umstände der gegenständlichen Übermittlung berücksichtigen. Dies sei für den gegenständlichen Fall relevant. Die Pseudonymisierung sei hier – in Einklang mit den EDSA-Leitlinien – eine wirksame ergänzende Maßnahme. Es sei nicht zu erwarten, dass US-Behörden über zusätzliche Informationen verfügten, die es ihnen ermöglichten, die hinter den First Party Cookie-Werten „gid“ und „cid“ oder hinter einer IP-Adresse stehenden betroffenen Personen zu identifizieren. Der Beschwerdeführer habe auch nicht die Feststellung beantragt, dass seine Rechte in der Vergangenheit verletzt worden seien.

A.10. Mit Stellungnahmen vom 9. Juli 2021 brachte der Beschwerdeführer zusammengefasst Folgendes vor:

Es sei eine Verarbeitung von personenbezogenen Daten gegeben, dies sei u.a. durch die vorgelegten Beilagen belegt. Wenn es letztlich für die Identifikation eines Website-Besuchers nur Voraussetzung sei, ob dieser gewisse Willenserklärungen in seinem Konto abgebe (wie etwa die Aktivierung von „Ad personalisation“), würden für den Zweitbeschwerdegegner alle Möglichkeiten der Identifizierbarkeit vorliegen. Andernfalls könne der Zweitbeschwerdegegner den in den Kontoeinstellungen ausgedrückten Wünschen eines Nutzers nach „Personalisierung“ der erhaltenen Werbeinformationen nicht entsprechen.

Der UUID (Universally Unique Identifier) im _gid-Cookie mit dem UNIX-Zeitstempel XY sei am Mittwoch, 12 August 2020 um 11:11 und 18 Sekunden MEZ gesetzt worden, jene im cid-Cookie mit dem UNIX-Zeitstempel YZ am Freitag, 14. August 2020 um 10:45 und 34 Sekunden MEZ. Daraus folge, dass diese Cookies schon vor dem beschwerdegegenständlichen Besuch verwendet worden seien und

auch ein längerfristiges Tracking stattgefunden habe. Der Beschwerdeführer habe seines Wissens diese Cookies auch nicht unmittelbar gelöscht und die Webseite www.xyz.at auch wiederholt besucht.

Der Zweitbeschwerdegegner verkenne das weite Verständnis der DSGVO bei der Beurteilung des Vorliegens personenbezogener Daten. Die konkret genutzte IP-Adresse sei auch für den Beschwerdeführer nicht mehr feststellbar. Dies sei aber irrelevant, da über die UUID in den Cookies ohnehin ein klarer Personenbezug bestehe. Speziell die Kombination von Cookie-Daten und IP-Adresse erlaube Tracking und die Auswertung von geografischer Lokalisation, Internet-Anschluss und Kontext des Besuchers, die mit den bereits beschriebenen Cookie-Daten verknüpfbar seien. Hierzu würden aber auch Daten wie der genutzte Browser, die Bildschirmauflösung oder das Betriebssystem („Device Fingerprinting“) kommen.

Im Rahmen der Beschwerde relevanter sei, dass US-Behörden gerade für Geheimdienste leicht feststellbare Daten, wie etwa die IP-Adresse, als Ausgangspunkt für die Überwachung von Einzelpersonen nutzen würden. Es sei das Standardvorgehen von Geheimdiensten, sich von einem Datum zu anderen „weiterzuhangeln“. Wenn der Computer des Beschwerdeführers etwa immer wieder über die IP-Adresse von NOYB im Internet auftauche, so könne dies genutzt werden, um die Arbeit des Vereins NOYB auszuspähen und um den Beschwerdeführer ins Visier zu nehmen. In einem weiteren Schritt würden dann andere Identifier in den Daten gesucht, wie etwa die genannten UUIDs, was wiederum eine Identifikation der einzelnen Person für eine Überwachung an anderen Orten ermögliche. Bei US-Geheimdiensten handle es sich in diesem Zusammenhang sohin um eine „andere Person“ im Sinne des Erwägungsgrundes 26 DSGVO. Der Beschwerdeführer arbeite nicht nur für NOYB, sondern habe als Musterbeschwerdeführer auch eine relevante Rolle in diesen Anstrengungen. Damit sei nach US-Recht eine Überwachung des Beschwerdeführers nach 50 USC § 1881a (ebenso wie von allen anderen mit dieser Beschwerde betrauten Personen) jederzeit legal möglich. Selbst bei der Anwendung des vermeintlichen „risikobasierten Ansatzes“ sei der gegenständliche Fall ein Paradebeispiel für ein hohes Risiko.

Die E-Mail-Adresse musteremail123@gmail.com sei dem Beschwerdeführer zuzuordnen, der bis zu einer Eheschließung den Nachnamen „Mustername“ getragen habe. Das alte Google-Konto werde jedoch noch immer benutzt. Es sei nicht erklärt, inwieweit die unstrittig vorliegenden Daten verknüpft, ausgewertet oder das Ergebnis einer Auswertung dem Nutzer nur nicht angezeigt werde.

Darüber hinaus kenne Kapitel V DSGVO keinen „risikobasierten Ansatz“. Dieser finde sich nur in bestimmten Artikeln der DSGVO, wie etwa in Art. 32 leg.cit. Die neuen Standardvertragsklauseln im Durchführungsbeschluss (EU) 2021/914 seien für den Sachverhalt mangels zeitlicher Gültigkeit nicht relevant. Eine „Übermittlung“ sei keine einseitige Handlung eines Datenexporteurs, jede „Übermittlung“ verlange auch einen Empfang der Daten. Demnach sei das Kapitel V der DSGVO auch für den Zweitbeschwerdegegner anwendbar, es handle sich um ein gemeinschaftliches Handeln von Datenexporteur und –importeur.

Selbst falls der Zweitbeschwerdegegner die Art. 44 ff DSGVO nicht verletzt habe, seien die Bestimmungen gemäß Art. 28 Abs. 3 lit. a und Art. 29 DSGVO als „Auffangregelung“ zu berücksichtigen. Leiste der Zweitbeschwerdegegner einer entsprechenden Weisung eines US-Geheimdienstes Folge, so treffe er damit die Entscheidung, personenbezogene Daten über den konkreten Auftrag der Erstbeschwerdegegnerin gemäß Art. 28 und Art. 29 DSGVO und den entsprechenden Vertragsdokumenten hinaus zu verarbeiten. Hierdurch werde der Zweitbeschwerdegegner gemäß Art. 28 Abs. 10 DSGVO selbst zum Verantwortlichen. Infolgedessen habe der Zweitbeschwerdegegner insbesondere auch die Bestimmungen der Art. 5 ff DSGVO zu befolgen. Eine heimliche Datenweitergabe an US-Geheimdienste gemäß dem Recht der USA sei ohne Zweifel nicht mit Art. 5 Abs. 1 lit. f DSGVO, Art. 5 Abs. 1 lit. a DSGVO und Art. 6 DSGVO vereinbar.

A.9. Mit letzter Stellungnahme vom 12. August 2021 brachte der Zweitbeschwerdegegner zusammengefasst Folgendes vor:

Der Beschwerdeführer habe seine Aktivlegitimation zur Beschwerdeeinbringung nicht dargetan. Er habe keine seitens des Zweitbeschwerdegegners aufgeworfenen Fragen zur Identifizierbarkeit seiner Person anhand der IP-Adresse beantwortet. In Bezug auf die _gid-Nummer und cid-Nummer sei festzuhalten, dass kein Verzeichnis vorhanden sei, um dadurch den Beschwerdeführer identifizierbar zu machen. Die Tatsache, dass in ErwGr 26 DSGVO das „Aussondern“ als mögliches Mittel zur Identifizierung erwähnt sei, ändere jedoch nicht das Verständnis der Worte „identifizieren“ oder „Identifizierung“ oder „Identifizierbarkeit“.

Die Identifizierbarkeit des Beschwerdeführers setze zumindest voraus, dass seine Identifizierung auf Grundlage der gegenständlichen Daten und mit Mitteln möglich sei, die nach allgemeinem Ermessen wahrscheinlich genutzt würden. Dies sei nicht festgestellt und könne nicht unterstellt werden und sei im Gegenteil sogar unwahrscheinlich, wenn nicht sogar unmöglich. Auch die Tatsache, dass der Zweitbeschwerdegegner Auftragsverarbeitervereinbarungen abgeschlossen habe, bedeute weder, dass es sich bei den Daten, die Gegenstand dieses Verfahrens seien, um personenbezogene Daten handle, noch, dass es sich um die Daten des Beschwerdeführers handle.

Der Ansicht des Beschwerdeführers, dass die Datenübermittlung nicht nach einem risikobasierten Ansatz zu bewerten sei („Alles-oder-Nichts“), sei nicht zu folgen. Dies stehe nicht im Einklang mit der DSGVO und sei an ErwGr 20 des Durchführungsbeschlusses (EU) 2021/914 der Europäischen Kommission zu sehen. Ebenso sei dies an den unterschiedlichen Versionen der EDSA-Empfehlung 01/2020 erkennbar. Selbst wenn ein Zugriff auf die oben angeführten Nummern durch US-Behörden „jederzeit legal“ möglich sei, sei zu überprüfen, wie wahrscheinlich dies sei. Der Beschwerdeführer habe keine überzeugenden Argumente dafür vorgebracht, warum oder wie die „Cookie-Daten“ im Zusammenhang mit seinem Besuch einer öffentlich zugänglichen, und von vielen genutzten österreichischen Website wie der in Rede stehenden, „Foreign Intelligence Information“ seien und damit zum Ziel der zweckbeschränkten Datenerfassung gemäß § 702 werden könnten.

B. Beschwerdegegenstand

Ausgehend vom Vorbringen des Beschwerdeführers ist erkennbar, dass Beschwerdegegenstand jedenfalls die Frage ist,

- ob die Erstbeschwerdegegnerin durch Implementierung des Tools Google Analytics auf ihrer Website www.xyz.at personenbezogene Daten des Beschwerdeführers an den Zweitbeschwerdegegner übermittelt hat und,
- ob für diese Datenübermittlung ein angemessenes Schutzniveau gemäß Art. 44 DSGVO gewährleistet wurde.

In diesem Zusammenhang ist auch zu klären, ob neben der Erstbeschwerdegegnerin (als Datenexporteurin) auch der Zweitbeschwerdegegner (als Datenimporteur) zur Einhaltung von Art. 44 DSGVO verpflichtet war.

Über den Antrag, gegen die Erstbeschwerdegegnerin (als Verantwortliche) nunmehr ein unverzügliches Verbot der Datenübermittlungen an den Zweitbeschwerdegegner zu verhängen, ist nicht abzusprechen, da – wie in Folge noch erläutert wird – die Zuständigkeit für den Betrieb der Website www.xyz.at im Laufe des Beschwerdeverfahrens (allerdings erst nach der beschwerderelevanten Datenübermittlung) auf die XYZ123 GmbH mit Sitz in Musterstadt übergegangen ist. In Bezug auf die Verhängung eines solchen Verbots hätte die Datenschutzbehörde den Fall an die zuständige deutsche Aufsichtsbehörde heranzutragen.

Ebenso nicht abzusprechen ist über den Antrag auf Verhängung einer Geldbuße, da dieser seitens des Beschwerdeführers mit Stellungnahme vom 5. Mai 2021 zurückgezogen wurde und dies nunmehr als Anregung zu verstehen ist.

Schließlich ist festzuhalten, dass mit dem gegenständlichen Teilbescheid nicht über die behaupteten Verstöße des Zweitbeschwerdegegners gemäß Art. 5 ff iVm Art. 28 Abs. 3 lit. a und Art. 29 DSGVO abgesprochen wird. Diesbezüglich sind noch weitere Ermittlungsschritte notwendig und wird hierüber in einem weiteren Bescheid abgesprochen.

C. Sachverhaltsfeststellungen

C.1. Die Erstbeschwerdegegnerin war jedenfalls am 14. August 2020 die Website-Betreiberin von www.xyz.at. Bei der österreichischen Version von „XYZ“ handelt es sich um ein Informationsportal zum Thema XY. Die Website www.xyz.at wird nur in deutscher Sprache angeboten. Die Erstbeschwerdegegnerin betrieb keine anderen Versionen der Website www.xyz.at in der EU. Die Erstbeschwerdegegnerin ist darüber hinaus nur in Österreich ansässig und besitzt keine weiteren Niederlassungen in anderen Ländern der EU. Für Deutschland gibt es eine deutsche Version von „XYZ“ unter www.XYZ.de, welche jedoch nicht seitens der Erstbeschwerdegegnerin betrieben wurde.

Beweiswürdigung zu C.1.: Die getroffenen Feststellungen beruhen auf der Stellungnahme des Erstbeschwerdegegners vom 16. Dezember 2020 (Frage 1 bis 3) und wurden insofern nicht seitens des Beschwerdeführers bestritten.

C.2. Zum 1. Februar 2021 wurde die Website www.xyz.at im Rahmen eines Asset-Deals auf die XYZ123 GmbH mit Sitz in Musterstadt übertragen. Im Anschluss wurde die Erstbeschwerdegegnerin von xyz123.at GmbH auf Neue Mustermann GmbH umbenannt. Die Erstbeschwerdegegnerin hat die Website www.xyz.at bis August 2021 für die XYZ123 GmbH betreut. Die Erstbeschwerdegegnerin ist seit August 2021 nicht mehr Betreiberin von www.xyz.at und trifft auch nicht mehr die Entscheidung darüber, ob das Tool Google Analytics zum Einsatz kommt.

Beweiswürdigung zu C.2.: Die getroffenen Feststellungen beruhen auf der Stellungnahme der Erstbeschwerdegegnerin vom 18. Juni 2021 und wurden insofern seitens des Beschwerdeführers nicht bestritten. Darüber hinaus beruhen die Feststellungen auf einer amtswegigen Recherche der Datenschutzbehörde im Firmenbuch zur Zl. FN xyz s.

C.3. Der Zweitbeschwerdegegner hat das Tool Google Analytics entwickelt. Bei Google Analytics handelt es sich um einen Messdienst, der es Kunden des Zweitbeschwerdegegners ermöglicht, Trafficigenschaften zu messen. Hierzu zählt auch die Messung des Traffics von Besuchern, die eine spezifische Website besuchen. Dadurch kann das Verhalten von Website-Besuchern nachvollzogen und gemessen werden, wie diese mit einer spezifischen Website interagieren. Konkret kann sich ein Website-Betreiber ein Google Analytics Konto anlegen und so mithilfe eines Dashboards Berichte zur Website betrachten. Ebenso kann mithilfe von Google Analytics die Wirksamkeit von Werbekampagnen, die Website-Besitzer auf Google-Anzeigendiensten durchführen, gemessen und optimiert werden.

Es gibt zwei Versionen von Google Analytics: Eine kostenlose Version sowie eine kostenpflichtige namens Google Analytics 360. Die kostenlose Version wurde seitens des Zweitbeschwerdegegners jedenfalls bis Ende April 2021 zur Verfügung gestellt. Seit Ende April 2021 werden beide Google Analytics Versionen von Google Ireland Limited bereitgestellt.

Beweiswürdigung zu C.3.: Die getroffenen Feststellungen beruhen auf der Stellungnahme des Zweitbeschwerdegegners vom 9. April 2021 (S. 3 sowie Frage 1 und 2) und wurden insofern nicht seitens des Beschwerdeführers bestritten.

C.4. Die Erstbeschwerdegegnerin – als Website-Betreiberin – hat jedenfalls zum Stichtag 14. August 2020 die Entscheidung getroffen, die kostenlose Version des Tools Google Analytics für die Website www.xyz.at einzusetzen. Hierzu hat sie einen JavaScript Code („tag“), der seitens des Zweitbeschwerdegegners zur Verfügung gestellt wird, im Quelltext ihrer Website eingebaut. Die Erstbeschwerdegegnerin hat das Tool eingesetzt, um allgemeine statistische Auswertungen über das

Verhalten von Website-Besuchern zu ermöglichen. Das Zusatztool Google Signals wurde nicht aktiviert.

Diese Auswertungen werden seitens der Erstbeschwerdegegnerin jedenfalls dazu genutzt, um den Inhalt der Website www.xyz.at entsprechend dem allgemeinen Themeninteresse so darzustellen, dass die auf die meiste Nachfrage stoßenden Channels in den Vordergrund gestellt und die Darstellung je nach Aktualität eines konkreten Themas angepasst werden kann.

Die Erstbeschwerdegegnerin hat hierzu ein Google Analytics Konto angelegt. Die Google Analytics Konto-ID mit dem Kontonamen „XYZ“ lautet ***. Die oben angeführten Auswertungen kann die Erstbeschwerdegegnerin vornehmen, indem sie sich in das „XYZ“ Google Analytics Konto einloggt und im Dashboard Berichte zum Traffic von www.xyz.at einsehen kann. Die Berichte gliedern sich in die Kategorien Echtzeit, Zielgruppe, Akquisition, Verhalten und Conversions. Die Erstbeschwerdegegnerin kann benutzerdefinierte Vorgaben für die Berichterstellung auswählen, der Zweitbeschwerdegegner nimmt hierauf keinen Einfluss. Der Zweitbeschwerdegegner nimmt auch keinen Einfluss darauf, inwiefern die Erstbeschwerdegegnerin die erstellten Berichte in weiterer Folge verwendet.

Das Dashboard gestaltet sich auszugsweise wie folgt (Formatierung nicht 1:1 wiedergegeben):

[Anmerkung Bearbeiter: Grafiken wurde entfernt]

Beweiswürdigung zu C.4.: Die getroffenen Feststellungen beruhen auf der Eingabe der Erstbeschwerdegegnerin vom 16. Dezember 2020 und wurden seitens des Beschwerdeführers nicht bestritten. Der angeführten Screenshots wurden aus Beilage ./1 und ./10 aufgenommen, die Darstellung der Berichterfassung ist in Beilage ./1 ausführlich dargelegt.

C.5. Das Tool Google Analytics hat folgende Funktionsweise: Wenn Besucher die Website www.xyz.at ansehen, verweist der im Quelltext der Website eingefügte JavaScript-Code auf eine zuvor auf das Gerät des Benutzers heruntergeladene JavaScript-Datei, die dann den Tracking-Betrieb für Google Analytics ausführt. Die Tracking-Operation ruft Daten über die Seitenanfrage mit verschiedenen Mitteln ab und sendet diese Informationen über eine Liste von Parametern an den Analytics-Server, die an eine einzelne Pixel-GIF-Bildanfrage angeschlossen ist.

Die Daten, die mithilfe von Google Analytics im Auftrag des Websitebetreibers erhoben werden, stammen aus folgenden Quellen:

- die HTTP-Anfrage des Benutzers;
- Browser/Systeminformationen;
- (First-Party) Cookies.

Eine HTTP-Anfrage für jede Website enthält Details über den Browser und den Computer, der die Anfrage stellt, wie etwa Hostname, Browsertyp, Referrer und Sprache. Darüber hinaus bietet die DOM-

Schnittstelle der Browser (die Schnittstelle zwischen HTML und dynamischem JavaScript) Zugriff auf detailliertere Browser- und Systeminformationen, wie Java- und Flash-Unterstützung und Bildschirmauflösung. Google Analytics nutzt diese Informationen. Google Analytics setzt und liest auch First-Party-Cookies auf Browsern eines Benutzers, die die Messung der Benutzersitzung und anderer Informationen aus der Seitenanfrage ermöglichen.

Wenn alle diese Informationen gesammelt werden, werden diese an die Analytics-Server in Form einer langen Liste von Parametern gesendet, die an eine einzelne GIF-Bildanfrage (die Bedeutung der GIF-Anfrageparameter wird hier beschrieben) an die Domain google-analytics.com gesendet werden. Die in der GIF-Anfrage enthaltenen Daten sind jene, die an die Analytics-Server gesendet und dann weiterverarbeitet werden und in den Berichten des Websitebetreibers enden.

Auf der Informationsseite des Zweitbeschwerdegegners zum Tool Google Analytics finden sich auszugsweise folgende Informationen (Formatierung nicht 1:1 wiedergegeben, abgefragt am 22. Dezember 2021):

gtag.js and analytics.js (Universal Analytics) - cookie usage

The [analytics.js JavaScript library](#) or the [gtag.js JavaScript library](#) can be used for [Universal Analytics](#). In both cases, the libraries use *first-party* cookies to:

- Distinguish unique users
- Throttle the request rate

When using the [recommended JavaScript snippet](#) cookies are set at the highest possible domain level. For example, if your website address is `blog.example.co.uk`, `analytics.js` and `gtag.js` will set the cookie domain to `.example.co.uk`. Setting cookies on the highest level domain possible allows measurement to occur across subdomains without any extra configuration.

★ **Note:** `gtag.js` and `analytics.js` do not require setting cookies to transmit data to Google Analytics.

`gtag.js` and `analytics.js` set the following cookies:

Cookie Name	Default expiration time	Description
<code>_ga</code>	2 years	Used to distinguish users.
<code>_gid</code>	24 hours	Used to distinguish users.
<code>_gat</code>	1 minute	Used to throttle request rate. If Google Analytics is deployed via Google Tag Manager, this cookie will be named <code>_dc_gtm_<property-id></code> .
<code>AMP_TOKEN</code>	30 seconds to 1 year	Contains a token that can be used to retrieve a Client ID from AMP Client ID service. Other possible values indicate opt-out, inflight request or an error retrieving a Client ID from AMP Client ID service.
<code>_gac_<property-id></code>	90 days	Contains campaign related information for the user. If you have linked your Google Analytics and Google Ads accounts, Google Ads website conversion tags will read this cookie unless you opt-out. Learn more .

Beweiswürdigung zu C.5.: Die getroffenen Feststellungen beruhen auf der Stellungnahme des Zweitbeschwerdegegners vom 9. April 2021 (Frage 2) sowie einer amtswegigen Recherche der Datenschutzbehörde unter <https://developers.google.com/analytics/devguides/collection/gajs/cookie-usage> sowie <https://developers.google.com/analytics/devguides/collection/gtagjs/cookies-user-id> (beide abgefragt am 22. Dezember 2021).

C.6. Erst- und Zweitbeschwerdegegner haben einen Vertrag mit dem Titel „Auftragsverarbeiterbedingungen für Google Werbeprodukte“ abgeschlossen. Dieser Vertrag hatte in der Version vom 12. August 2020 zumindest am 14. August 2020 Gültigkeit. Der Vertrag regelt Auftragsverarbeitungsbedingungen für „Google Werbeprodukte“. Er gilt für die Bereitstellung von Auftragsverarbeiterdiensten und damit im Zusammenhang stehende technischen Supportleistungen für Kunden des Zweitbeschwerdegegners. Der genannte Vertrag in der Version vom 12. August 2020 (Beilage ./7) wird den Sachverhaltsfeststellungen zugrunde gelegt.

Darüber hinaus haben Erst- und Zweitbeschwerdegegner am 12. August 2020 einen zweiten Vertrag

mit dem Titel „Google Ads Data Processing Terms: Model Contract Clauses, Standard Contractual Clauses for Processors“ abgeschlossen. Dabei handelt es sich um Standardvertragsklauseln für den internationalen Datenverkehr. Auch der genannte zweite Vertrag in der Version vom 12. August 2020 (Beilage ./11) wird den Sachverhaltsfeststellungen zugrunde gelegt.

Hinsichtlich der in Anhang 1 des zweiten Vertrags angeführten Datenkategorien wird auf den Link <https://privacy.google.com/businesses/adsservices/> verwiesen. Unter dem genannten Link wird auszugswise Folgendes angezeigt (rote Hervorhebung seitens der Datenschutzbehörde, Formatierung nicht 1:1 wiedergegeben, abgefragt am 22. Dezember 2021):

Auftragsdatenverarbeitungsbedingungen:

Auftragsverarbeiterdienste

Die folgenden Google-Dienste fallen unter den Anwendungsbereich der Auftragsdatenverarbeitungsbedingungen für Google Werbeprodukte:

- Ads Data Hub
- Audience Partner API (frühere Bezeichnung: DoubleClick Data Platform)
- Campaign Manager 360 (frühere Bezeichnung: Campaign Manager)
- Display & Video 360 (frühere Bezeichnung: DoubleClick Bid Manager)
- Erweiterte Conversions
- [Google Ad Manager-Auftragsverarbeiterfunktionen](#)
- [Google Ad Manager 360-Auftragsverarbeiterfunktionen](#)
- Google Ads Kundenabgleich
- Google Ads Ladenverkäufe (direkter Upload)
- Google Analytics
- Google Analytics 360
- Google Analytics für Firebase
- Google Data Studio
- Google Optimize
- Google Optimize 360
- Google Tag Manager
- Google Tag Manager 360
- Search Ads 360 (frühere Bezeichnung: DoubleClick Search)

Google ist berechtigt, diese Liste gemäß den Bestimmungen der Auftragsdatenverarbeitungsbedingungen für Google Werbeprodukte zu aktualisieren.

Arten personenbezogener Daten

In Bezug auf die Auftragsdatenverarbeitungsbedingungen für Google Werbeprodukte (und abhängig davon, welche Auftragsverarbeiterdienste unter der jeweiligen Vereinbarung genutzt werden) können die folgenden Arten personenbezogener Daten personenbezogene Daten des Kunden darstellen:

Auftragsverarbeiterdienste	Arten personenbezogener Daten
Ads Data Hub	Online-Kennzeichnungen (einschließlich Cookie-Kennungen), Internet-Protokoll-Adressen und Gerätekennungen, vom Kunden vergebene Kennzeichnungen
Audience Partner API (frühere Bezeichnung: DoubleClick Data Platform)	Online-Kennzeichnungen (einschließlich Cookie-Kennungen) und Gerätekennungen
Campaign Manager 360 (frühere Bezeichnung: Campaign Manager)	Online-Kennzeichnungen (einschließlich Cookie-Kennungen), Internet-Protokoll-Adressen und Gerätekennungen, präzise Standortdaten, vom Kunden vergebene Kennzeichnungen
Display & Video 360	Online-Kennzeichnungen (einschließlich Cookie-Kennungen), Internet-Protokoll-Adressen und Gerätekennungen, präzise Standortdaten, vom Kunden vergebene Kennzeichnungen
Erweiterte Conversions	Namen, E-Mail-Adressen, Telefonnummern, Adressen, vom Kunden bereitgestellte Kennzeichnungen, Online-Kennzeichnungen (einschließlich Internet-Protokoll-Adressen)
Google Ad Manager-Auftragsverarbeiterfunktionen	Verschlüsselte Signale
Google Ad Manager 360-Auftragsverarbeiterfunktionen	Verschlüsselte Signale
Google Ads Kundenabgleich	Namen, E-Mail-Adressen, Adressen und vom Partner bereitgestellte Kennzeichnungen
Google Ads Ladenverkäufe (direkter Upload)	Namen, E-Mail-Adressen, Telefonnummern und Adressen
Google Analytics	Online-Kennzeichnungen (einschließlich Cookie-Kennungen), Internet-Protokoll-Adressen und Gerätekennungen, vom Kunden vergebene Kennzeichnungen
Google Analytics 360	Online-Kennzeichnungen (einschließlich Cookie-Kennungen), Internet-Protokoll-Adressen und Gerätekennungen, vom Kunden vergebene Kennzeichnungen

Zusätzlich zum Abschluss von Standardvertragsklauseln hat der Zweitbeschwerdegegner weitere vertragliche, organisatorische und technische Maßnahmen implementiert. Diese Maßnahmen ergänzen die in den Standardvertragsklauseln enthaltenen Verpflichtungen. Die Maßnahmen werden in der Stellungnahme des Zweitbeschwerdegegners vom 9. April 2021, Frage 28 beschrieben. Diese Beschreibung wird den Sachverhaltsfeststellungen zugrunde gelegt.

Der Zweitbeschwerdegegner veröffentlicht regelmäßig sogenannte Transparenzberichte („Transparency Reports“) zu Datenanfragen von US-Behörden. Diese sind abrufbar unter:

<https://transparencyreport.google.com/user-data/us-national-security?hl=en>

Beweiswürdigung zu C.6.: Die getroffenen Feststellungen beruhen auf der Stellungnahme des Erstbeschwerdegegners vom 16. Dezember 2020, Frage 15. Die angeführte Beilage ./7 sowie ./11 sind im Akt enthalten und allen Beteiligten bekannt. Darüber hinaus beruhen die getroffenen Feststellungen auf einer amtswegigen Recherche der Datenschutzbehörde unter <https://privacy.google.com/businesses/adsservices/> (abgefragt am 22. Dezember 2021). Die getroffenen Feststellungen im Hinblick auf die „zusätzlich implementierten Maßnahmen“ ergeben sich aus der Stellungnahme des Zweitbeschwerdegegners vom 9. April 2021 (Frage 28). Die Stellungnahme des Zweitbeschwerdegegners vom 9. April 2021 ist im Akt enthalten und ist allen Beteiligten bekannt. Die Feststellung im Hinblick auf die Transparenzberichte ergibt sich aus einer amtswegigen Recherche der Datenschutzbehörde unter <https://transparencyreport.google.com/user-data/us-national-security?hl=en> (abgefragt am 22. Dezember 2021).

C.7. Im Zuge der Verwendung des Tools Google Analytics wird die Möglichkeit angeboten, eine „IP-Anonymisierungsfunktion“ zu verwenden. Diese Funktion wurde jedenfalls am 14. August 2020 nicht korrekt auf www.xyz.at implementiert.

Beweiswürdigung zu C.7.: Die getroffenen Feststellungen beruhen auf der Stellungnahme der Erstbeschwerdegegnerin vom 18. Juni 2021. Darin räumt diese ein, dass die genannte „IP-Anonymisierungsfunktion“ aufgrund eines Codefehlers nicht ordnungsgemäß implementiert wurde.

C.8. Der Beschwerdeführer besuchte zumindest am 14. August 2020, um 10:45 Uhr, die Website www.xyz.at. Während des Besuchs war er in seinem Google-Konto eingeloggt, welches mit der E-Mail-Adresse musteremail123@gmail.com verknüpft ist. Die E-Mail-Adresse gehört dem Beschwerdeführer. Der Beschwerdeführer hatte in der Vergangenheit den Nachnamen „Mustername“.

Bei einem Google-Konto handelt es sich um ein Benutzerkonto, welches zur Authentifizierung bei verschiedenen Google-Onlinediensten des Zweitbeschwerdegegners dient. So ist ein Google-Konto etwa Voraussetzung für die Nutzung von Diensten wie „Gmail“ oder „Google Drive“ (ein Filehosting-Dienst).

Beweiswürdigung zu C.8.: Die getroffenen Feststellungen beruhen auf der Eingabe des Beschwerdeführers vom 18. August 2020 (S. 3) und wurden seitens der Beschwerdegegner nicht bestritten. Die getroffenen Feststellungen im Hinblick auf die grundsätzlichen Funktionen eines Google-Kontos beruhen auf einer amtswegigen Recherche der Datenschutzbehörde unter <https://support.google.com/accounts/answer/27441?hl=de> sowie <https://policies.google.com/privacy> (beide abgefragt am 22. Dezember 2021).

C.9. In der Transaktion zwischen dem Browser des Beschwerdeführers und <https://tracking.XYZ123.at/> wurden am 14. August 2020, um *** MEZ einzigartige Nutzer-Identifikations-Nummern zumindest in den Cookies „_ga“ und „_gid“ gesetzt. In Folge wurden diese Kennnummern am 14. August 2020, um *** MEZ an <https://www.google-analytics.com/> und somit an den Zweitbeschwerdegegner übermittelt.

Konkret wurden folgende Nutzer-Identifikations-Nummern, die sich im Browser des Beschwerdeführers befinden, an den Zweitbeschwerdegegner übermittelt (gleiche Werte, die jeweils in verschiedenen Transaktionen aufgetreten sind, wurden jeweils farblich mit orange und grün gekennzeichnet):

[Anmerkung Bearbeiter: Grafik wurde entfernt]

Diese Kennnummern enthalten jeweils am Ende einen UNIX-Zeitstempel, aus dem sich ergibt, wann das jeweilige Cookie gesetzt wurde. Die Kennnummer im _gid-Cookie mit dem UNIX-Zeitstempel „1234***“ wurde am Mittwoch, 14. August 2020, um *** MEZ gesetzt, jene im cid-Cookie mit dem UNIX-Zeitstempel „4321***“ am Freitag, 12 August 2020, um *** MEZ.

Mithilfe dieser Kennnummern ist es für die Beschwerdegegner möglich, Website-Besucher zu unterscheiden und auch die Information zu erhalten, ob es sich um einen neuen oder um einen wiederkehrenden Website-Besucher von www.xyz.at handelt.

Darüber hinaus wurden jedenfalls auch folgende Informationen (Parameter) über den Browser des Beschwerdeführers im Zuge von Anfragen (Requests) an <https://www.google-analytics.com/collect> an den Zweitbeschwerdegegner übermittelt (Auszug aus der HAR-Datei, Request URL <https://www.google-analytics.com/collect>, Auszug der Anfrage mit Zeitstempel ****):

[Anmerkung Sachbearbeiter: Informationen zu den Browserdaten wurden entfernt]

Aus diesen Parametern können somit Rückschlüsse auf den verwendeten Browser, die Browsereinstellungen, Sprachauswahl, die besuchte Website, die Farbtiefe, die Bildschirmauflösung und die AdSense-Linking-Nummer gezogen werden.

Bei der Remote Adresse *** handelt es sich um jene des Zweitbeschwerdegegners.

Die IP-Adresse des Geräts des Beschwerdeführers wird im Rahmen dieser Anfragen an <https://www.google-analytics.com/collect> an den Zweitbeschwerdegegner übermittelt.

Der Inhalt der HAR-Datei (Beilage ./4), welche seitens des Beschwerdeführers mit Eingabe vom 18. August 2020 vorgelegt wurde, wird den Sachverhaltsfeststellungen zugrunde gelegt.

*Beweiswürdigung zu C.9.: Die getroffenen Feststellungen beruhen auf der Eingabe des Beschwerdeführers vom 18. August 2020 und der darin vorgelegten HAR-Datei, Beilage ./4. Bei einer HAR-Datei handelt es sich um ein Archivformat für HTTP-Transaktionen. Die HAR-Datei wurde seitens der Datenschutzbehörde überprüft. Das Vorbringen des Beschwerdeführers stimmt mit den darin enthaltenen Archivdaten überein. Die vorgelegte HAR-Datei (bzw. deren Inhalt) ist den Beteiligten bekannt. Darüber hinaus beruhen die getroffenen Feststellungen auf der Stellungnahme des Beschwerdeführers vom 5. Mai 2021 (S. 8 ff) und den darin enthaltenen Screenshots. Wie bereits oben ausgeführt, liegt nach Angaben des Zweitbeschwerdegegners der Zweck der Kennnummern darin, Benutzer zu unterscheiden. Die festgestellten Zeitpunkte der Cookiesetzung errechnen sich aus den jeweiligen UNIX-Zeitstempeln. Die Unixzeit ist eine Zeitdefinition, die für das Betriebssystem Unix entwickelt und als POSIX-Standard festgelegt wurde. Die Unixzeit zählt die vergangenen Sekunden seit Donnerstag, dem 1. Jänner 1970, 00:00 Uhr UTC. Die Feststellung im Hinblick auf die Remote-Adresse ergibt sich aus einer amtswegigen Who-Is-Abfrage der Datenschutzbehörde unter [https://who.is/whois-ip/ip-address/***\(abgefragt am 22. Dezember 2021\)](https://who.is/whois-ip/ip-address/***(abgefragt am 22. Dezember 2021)).*

C.10. Soweit das Tool Google Analytics auf einer Website implementiert ist, hat der Zweitbeschwerdegegner die technische Möglichkeit, die Information zu bekommen, dass ein bestimmter Google-Account-Nutzer diese Website (auf der Google Analytics implementiert ist) besucht

hat, sofern dieser Google-Account-Nutzer während des Besuchs im Google Konto eingeloggt ist.

Beweiswürdigung zu C.10.: In seiner Stellungnahme vom 9. April 2021 hat der Zweitbeschwerdegegner bei Frage 9 zwar vorgebracht, dass er eine derartige Information nur bekommt, wenn gewisse Voraussetzungen erfüllt sind, wie etwa die Aktivierung von spezifischen Einstellungen im Google-Account. Nach Auffassung der Datenschutzbehörde vermag dieses Vorbringen nicht zu überzeugen. Wenn nämlich dem Wunsch eines Google-Account-Nutzers nach „Personalisierung“ der erhaltenen Werbeinformationen aufgrund einer Willenserklärung im Konto entsprochen werden kann, so besteht aus rein technischer Sicht die Möglichkeit, die Information über die besuchte Website des Google-Account-Nutzers zu erhalten. In diesem Zusammenhang ist ausdrücklich auf die datenschutzrechtliche Rechenschaftspflicht hinzuweisen, auf welche im Rahmen der rechtlichen Beurteilung näher eingegangen wird. Für die Sachverhaltsfeststellung bedeutet diese datenschutzrechtliche Rechenschaftspflicht, dass die Beschwerdegegner (bzw. jedenfalls die Erstbeschwerdegegnerin als Verantwortliche) – und nicht der Beschwerdeführer oder die Datenschutzbehörde – einen ausreichenden Beweis erbringen muss. Ein solch ausreichender Beweis – also, dass aus technischer Sicht keine Möglichkeit des Datenerhalts für den Zweitbeschwerdegegner besteht – wurde in diesem Zusammenhang nicht erbracht, zumal es gerade ein wesentlicher Bestandteil des Konzepts von Google Analytics ist, auf möglichst vielen Websites implementiert zu werden, um Daten sammeln zu können.

C.11. Die Erstbeschwerdegegnerin hat den Zweitbeschwerdegegner im Laufe des Verfahrens angewiesen, alle über die Google Analytics Properties gesammelten Daten für die Website www.xyz.at zu löschen. Der Zweitbeschwerdegegner hat die Löschung bestätigt.

Beweiswürdigung zu C.11.: Die getroffenen Feststellungen beruhen auf der Stellungnahme der Erstbeschwerdegegnerin vom 18. und 24. Juni 2021 sowie der vorgelegten Kopie der Korrespondenz zwischen Erst- und Zweitbeschwerdegegner.

D. In rechtlicher Hinsicht folgt daraus:

D.1. Allgemeines

a) Zur Zuständigkeit der Datenschutzbehörde

Der Europäische Datenschutzausschuss (in Folge: EDSA) hat sich bereits mit dem Verhältnis zwischen DSGVO und Richtlinie 2002/58/EG („e-Datenschutz-RL“) auseinandergesetzt (vgl. die Stellungnahme 5/2019 zum Zusammenspiel zwischen der e-Datenschutz-RL und der DSGVO vom 12. März 2019).

Auch die Datenschutzbehörde hat sich mit Bescheid vom 30. November 2018, Zl. DSB-D122.931/0003-DSB/2018, mit dem Verhältnis zwischen DSGVO und der nationalen

Umsetzungsbestimmung (in Österreich nunmehr: TKG 2021, BGBl. I Nr. 190/2021 idgF) auseinandergesetzt.

Dabei wurde grundsätzlich festgehalten, dass die e-Datenschutz-RL (bzw. die jeweils nationale Umsetzungsbestimmung) der DSGVO als *lex specialis* vorgeht. So normiert Art. 95 DSGVO, dass 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.

In der e-Datenschutz-RL finden sich jedoch keine Pflichten im Sinne von Kapitel V der DSGVO für den Fall der Übermittlung von personenbezogenen Daten an Drittländer oder an internationale Organisationen.

Festzuhalten ist an dieser Stelle erneut, dass die Zuständigkeit für den Betrieb der Website www.xyz.at erst nach der beschwerderelevanten Datenübermittlung am 14. August 2020 auf eine deutsche Gesellschaft übergegangen ist.

Vor diesem Hintergrund ist auf eine solche Datenübermittlung die DSGVO anzuwenden und besteht somit eine Zuständigkeit der Datenschutzbehörde zur Behandlung der gegenständlichen Beschwerde nach Art. 77 Abs. 1 DSGVO.

b) Zu Art. 44 DSGVO als subjektives Recht

Ausgehend von der bisherigen Spruchpraxis der Datenschutzbehörde und der Gerichte ist festzuhalten, dass sowohl die Rechtmäßigkeit der Datenverarbeitung nach Art. 5 Abs. 1 lit. a iVm Art. 6 ff DSGVO als auch die in Kapitel III der Verordnung postulierten datenschutzrechtlichen Betroffenenrechte als subjektives Recht im Rahmen einer Beschwerde nach Art. 77 Abs. 1 DSGVO geltend gemacht werden können.

Die Übermittlung von personenbezogenen Daten in ein Drittland, welches im Sinne des Art. 44 DSGVO (behauptetermaßen) kein angemessenes Schutzniveau gewährleistet, war bislang noch nicht Beschwerdegegenstand im Rahmen eines Beschwerdeverfahrens vor der Datenschutzbehörde.

In diesem Zusammenhang ist festzuhalten, dass Art. 77 Abs. 1 DSGVO (und im Übrigen auch die nationale Bestimmung des § 24 Abs. 1 DSG) für die Inanspruchnahme des Beschwerderechts nur voraussetzt, dass „[...] die Verarbeitung der sie betreffenden personenbezogenen Daten gegen diese Verordnung verstößt“.

Auch der EuGH ist in seinem Urteil vom 16. Juli 2020 davon ausgegangen, dass die Feststellung, dass „[...] das Recht und die Praxis eines Landes kein angemessenes Schutzniveau gewährleisten [...]“ sowie „[...] die Vereinbarkeit dieses (Angemessenheits-) Beschlusses mit dem Schutz der Privatsphäre

sowie der Freiheiten und Grundrechte von Personen [...]“ im Rahmen einer Beschwerde nach Art. 77 Abs. 1 DSGVO als subjektives Recht geltend gemacht werden kann (vgl. das Urteil des EuGH vom 16. Juli 2020, C-311/18 Rz 158).

Zwar ist festzuhalten, dass die Vorlagefrage des genannten Verfahrens nicht den „Umfang des Beschwerderechts von Art. 77 Abs. 1 DSGVO“ zum Gegenstand hatte; der EuGH hat aber den Umstand, dass auch ein Verstoß gegen Bestimmungen von Kapitel V DSGVO im Rahmen einer Beschwerde nach Art. 77 Abs. 1 DSGVO geltend gemacht werden kann, offenkundig als notwendige Voraussetzung erachtet. Bei anderer Betrachtung hätte der EuGH wohl ausgesprochen, dass die Frage der Gültigkeit eines Angemessenheitsbeschlusses im Rahmen eines Beschwerdeverfahrens gar nicht geklärt werden kann.

Soweit der Zweitbeschwerdegegner darüber hinaus die Geltendmachung von Art. 44 DSGVO als subjektives Recht – unter Verweis auf den Wortlaut von ErwGr 141 leg.cit. – in Abrede stellt, ist dem zu entgegen, dass der genannte ErwGr daran anknüpft, dass die „Rechte gemäß dieser Verordnung“ einer Beschwerde nach Art. 77 Abs. 1 DSGVO zugänglich sind (und nicht etwa: „die Rechte nach Kapitel III dieser Verordnung“).

Zwar wird in der DSGVO an gewissen Stellen der Begriff „Rechte einer betroffenen Person“ verwendet, dies bedeutet aber im Umkehrschluss nicht, dass nicht auch andere Normen, in denen diese Formulierung nicht gewählt wird, als subjektives Recht geltend gemacht werden können. Die meisten Bestimmungen der DSGVO sind nämlich einerseits eine Verpflichtung des Verantwortlichen (und teils des Auftragsverarbeiters), können aber andererseits auch als subjektives Betroffenenrecht geltend gemacht werden. So ist etwa unstrittig, dass Art. 13 und Art. 14 DSGVO ein subjektives Informationsrecht begründen, obwohl das Informationsrecht nicht in Art. 12 Abs. 2 leg. cit. als „ihre Rechte“ (also „Rechte des Betroffenen“) angeführt wird und Art. 13 und Art. 14 DSGVO dem Wortlaut nach als Informationspflicht des Verantwortlichen konzipiert sind.

Entscheidend ist, ob eine betroffene Person durch eine behauptete Rechtsverletzung in einer individuellen Rechtsposition beeinträchtigt wird. Die behauptete Rechtsverletzung muss sich daher negativ auf die betroffene Person auswirken und sie beeinträchtigen.

Abgesehen davon sind die ErwGr zwar ein wichtiges Instrument zur Auslegung der DSGVO, allerdings können sie nicht dazu verwendet werden, um zu einem mit dem Verordnungstext im Widerspruch stehenden Ergebnis (hier wie oben ausgeführt der Umstand, dass der verwaltungsrechtliche Rechtsbehelf allgemein an „die Verarbeitung“ anknüpft) zu gelangen (vgl. das Urteil des EuGH vom 12. Mai 2005, C-444/03 Rz 25 und die dort angeführte weitere Judikatur).

Schließlich ist auch nach innerstaatlicher Judikatur des VwGH im Zweifel davon auszugehen, dass Normen, die ein behördliches Vorgehen auch und gerade im Interesse des Betroffenen vorschreiben,

diesem ein subjektives, also im Beschwerdeweg durchsetzbares Recht einräumen (vgl. etwa VwSlg. 9151 A/1976, 10.129 A/1980, 13.411 A/1991, 13.985 A/1994).

Vor dem Hintergrund des Wortlauts von Art. 77 Abs. 1 DSGVO sowie der angeführten Judikatur des EuGH und des VwGH ist als Zwischenergebnis festzuhalten, dass die in Kapitel V und insbesondere die in Art. 44 DSGVO normierte Verpflichtung für Verantwortliche und Auftragsverarbeiter, das durch die Verordnung gewährleistete Schutzniveau für natürliche Personen sicherzustellen, umgekehrt auch als subjektives Recht vor der zuständigen Aufsichtsbehörde gemäß Art. 77 Abs. 1 DSGVO geltend gemacht werden kann.

c) Zur Feststellungskompetenz der Datenschutzbehörde

Nach der Judikatur des VwGH und des BVwG kommt der Datenschutzbehörde eine Feststellungskompetenz im Hinblick auf Verletzungen des Rechts auf Geheimhaltung in Beschwerdeverfahren zu (so ausdrücklich das Erkenntnis des BVwG vom 20. Mai 2021, ZI. W214 222 6349-1/12E; implizit das Erkenntnis des VwGH vom 23. Februar 2021, Ra 2019/04/0054, worin sich dieser mit der Feststellung einer in der Vergangenheit liegenden Geheimhaltungspflichtverletzung auseinandergesetzt hat, ohne die Unzuständigkeit der belangten Behörde aufzugreifen).

Es bestehen keine sachlichen Gründe, die Feststellungskompetenz gemäß Art. 58 Abs. 6 DSGVO iVm § 24 Abs. 2 Z 5 DSGVO und Abs. 5 DSG nicht auch für die Feststellung einer Verletzung von Art. 44 DSGVO heranzuziehen, da auch im gegenständlichen Fall u.a. eine in der Vergangenheit liegende Rechtsverletzung – nämlich eine Datenübermittlung in die USA – moniert wird und das Beschwerderecht gemäß § 24 Abs. 1 DSG – ebenso wie Art. 77 Abs. 1 DSGVO – allgemein an einen Verstoß gegen die DSGVO anknüpft. Wenn der Spruch eines Bescheids in einem Beschwerdeverfahren nämlich ausschließlich Anweisungen nach Art. 58 Abs. 2 DSGVO enthalten könnte, wäre im Ergebnis kein Raum für § 24 Abs. 2 Z 5 und 24 Abs. 5 DSG.

Entgegen der Auffassung der Beschwerdegegner kommt § 24 Abs. 6 DSG für den hier relevanten Beschwerdegegenstand nicht in Betracht, da eine Datenübermittlung in der Vergangenheit moniert wird. Mit anderen Worten: Die behauptete Unrechtmäßigkeit (hier: Unvereinbarkeit mit Art. 44 DSGVO) einer bereits abgeschlossenen Datenübermittlung ist einem Verfahrensabschluss gemäß § 24 Abs. 6 DSG nicht zugänglich.

Vor dem Hintergrund dieser Ausführungen ist als weiteres Zwischenergebnis festzuhalten, dass die Feststellungskompetenz der Datenschutzbehörde im gegenständlichen Beschwerdeverfahren gegeben ist.

D.2. Spruchpunkt 1

Wie festgestellt, setzte die Datenschutzbehörde das gegenständliche Verfahren mit Bescheid vom 2. Oktober 2020, Zl. D155.027, 2020-0.527.385, bis zur Feststellung, welche Behörde für die inhaltliche Verfahrensführung zuständig ist (federführende Aufsichtsbehörde) bzw. bis zur Entscheidung einer federführenden Aufsichtsbehörde oder des EDSA, aus.

Ausgehend von den nunmehrigen Ermittlungsergebnissen ist festzuhalten, dass eine grenzüberschreitende Datenverarbeitung im Sinne der Art. 4 Z 23 iVm Art. 56 Abs. 1 DSGVO in Bezug auf den Beschwerdegegenstand – eine Datenübermittlung in die USA im August 2020 – nicht vorliegt und der „One-Stop-Shop“ - Mechanismus gemäß Art. 60 DSGVO daher hierfür keine Anwendung findet:

So ist der Erstbeschwerdegegner laut eigenen Angaben (vgl. Stellungnahme vom 16. Dezember 2020, Frage 2) weder in mehr als einem Mitgliedstaat niedergelassen (eine Datenverarbeitung im Sinne des Art. 4 Z 23 lit. a DSGVO im Rahmen der Tätigkeit von Niederlassungen in mehr als einem Mitgliedsstaat kann daher nicht vorliegen), noch hat die Datenübermittlung und damit die Verarbeitung personenbezogener Daten des Erstbeschwerdegegners erhebliche Auswirkungen auf betroffene Personen in mehr als einem Mitgliedstaat (Art. 4 Z 23 lit. b leg. cit.).

Im Hinblick auf die Auswirkungen der gegenständlichen Datenverarbeitung ergibt sich aus den Sachverhaltsfeststellungen, dass das Zielpublikum der hier relevanten Website www.xyz.at nämlich (primär) in Österreich niedergelassene Personen sind, auch weil es mit der Website www.XYZ.de eine eigene Version für das deutsche Publikum gibt. Laut Angaben der Erstbeschwerdegegnerin (vgl. die Stellungnahme vom 16. Dezember 2020, Frage 2) war dieser (jedenfalls im August 2020) nur für die österreichische Version von www.xyz.at verantwortlich.

Die theoretische Möglichkeit, dass deutschsprachige Personen aus einem anderen Mitgliedstaat als Österreich auf www.xyz.at zugreifen können, vermag den Tatbestand „Auswirkungen auf betroffene Personen in mehr als einem Mitgliedstaat“ gemäß Art. 4 Z 23 lit. b DSGVO nicht zu begründen. Bei einer davon abweichenden Betrachtung wäre jede Beschwerde gegen den Betreiber einer Website – unabhängig vom intendierten Zielpublikum der Website – gemäß den Regeln nach Art. 60 ff DSGVO zu behandeln. Dies würde zu einer zu weiten Interpretation von Art. 4 Z 23 lit. b DSGVO (und folglich zu einem zu weiten Anwendungsbereich des „One-Stop-Shop“) führen, was – nach Auffassung der Datenschutzbehörde – vom Ordnungsgeber nicht gewollt sein kann.

Folgerichtig war die Beschwerde in Bezug auf den hier relevanten Beschwerdegegenstand ausschließlich von der österreichischen Datenschutzbehörde gemäß Art. 55 Abs. 1 DSGVO zu behandeln.

Da von Amts wegen Bescheide, aus denen niemandem ein Recht erwachsen ist, sowohl von der Behörde, die den Bescheid erlassen hat, als auch in Ausübung des Aufsichtsrechtes von der sachlich in Betracht kommenden Oberbehörde aufgehoben oder abgeändert werden können, und infolge einer Verfahrensaussetzung einer Partei des Verfahrens kein Recht auf Nichtentscheidung entsteht, war der oben angeführte Bescheid vom 2. Oktober 2020 einer Behebung gemäß § 68 Abs. 2 AVG zugänglich.

D.2. Spruchpunkt 2. a)

a) Allgemeines zum Begriff „personenbezogene Daten“

Der sachliche Anwendungsbereich des Art. 2 Abs. 1 DSGVO – und somit der Erfolg dieser Beschwerde – setzt grundlegend voraus, dass „personenbezogene Daten“ verarbeitet werden.

Gemäß der Legaldefinition des Art. 4 Z 1 DSGVO sind „personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann“.

Wie sich aus den Sachverhaltsfeststellungen ergibt (vgl. Punkt C.9.), hat die Erstbeschwerdegegnerin – als Betreiberin der Website – das Tool Google Analytics auf ihrer Website implementiert. Als Folge dieser Implementierung – also ausgelöst durch den beim Websitebesuch ausgeführten JavaScript Code – wurden zumindest folgende Informationen vom Browser des Beschwerdeführers, der die Website www.xyz.at besucht hat, an die Server des Zweitbeschwerdegegners übermittelt:

- einzigartige Online-Kennungen („unique identifier“), die sowohl den Browser bzw. das Gerät des Beschwerdeführers als auch den Erstbeschwerdegegner (durch die Google Analytics Account ID des Erstbeschwerdegegners als Websitebetreiber) identifizieren;
- die Adresse und den HTML-Titel der Website sowie die Unterseiten, die der Beschwerdeführer besucht hat;
- Informationen zum Browser, Betriebssystem, Bildschirmauflösung, Sprachauswahl sowie Datum und Uhrzeit des Website-Besuchs;
- die IP-Adresse des Geräts, welches der Beschwerdeführer verwendet hat.

Zu überprüfen ist, ob diese Informationen unter die Definition von Art. 4 Z 1 DSGVO fallen, es sich also um personenbezogene Daten des Beschwerdeführers handelt.

b) Kennnummern als „personenbezogene Daten“

Im Hinblick auf die Online-Kennungen ist erneut in Erinnerung zu rufen, dass die gegenständlichen Cookies „_ga“ bzw. „cid“ (Client ID) und „_gid“ (User ID) einzigartige Google Analytics Kennnummern enthalten und auf dem Endgerät bzw. im Browser des Beschwerdeführers abgelegt wurden. Wie festgestellt, ist es gewissen Stellen – hier etwa den Beschwerdegegnern – möglich, mithilfe dieser Kennnummern Website-Besucher zu unterscheiden und auch die Information zu erhalten, ob es sich um einen neuen oder um einen wiederkehrenden Website-Besucher von www.xyz.at handelt. Mit anderen Worten: Erst der Einsatz solcher Kennnummern ermöglicht eine Unterscheidung von Website-Besuchern, die vor dieser Zuordnung nicht möglich war.

Nach Auffassung der Datenschutzbehörde liegt ein Eingriff in das Grundrecht auf Datenschutz gemäß Art. 8 EU-GRC sowie § 1 DSGVO bereits dann vor, wenn gewisse Stellen Maßnahmen setzen – hier die Zuordnung solcher Kennnummern – um Website-Besucher derart zu individualisieren.

Ein Maßstab an die „Identifizierbarkeit“ dahingehend, dass es sofort möglich sein muss, solche Kennnummern auch mit einem bestimmten „Gesicht“ einer natürlichen Person – also insbesondere mit dem Namen des Beschwerdeführers – in Verbindung zu bringen, ist nicht geboten (vgl. hierzu bereits die Stellungnahme 4/2007, WP 136, 01248/07/DE der ehemaligen Art. 29-Datenschutzgruppe zum Begriff „personenbezogene Daten“ S. 16 f; vgl. die Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien aus März 2019, S. 15).

Für eine solche Auslegung spricht ErwGr 26 DSGVO, wonach bei der Frage, ob eine natürliche Person identifizierbar ist, „[...] *alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern*“ (englische Sprachfassung der Verordnung: „singling out“). Unter dem Begriff „Aussondern“ ist das „Heraussuchen aus einer Menge“ zu verstehen (vgl. <https://www.duden.de/rechtschreibung/aussondern>, abgefragt am 22. Dezember 2021), was den oben angeführten Überlegungen zur Individualisierung von Website-Besuchern entspricht.

In der Literatur wird ebenso ausdrücklich vertreten, dass bereits ein „digitaler Fußabdruck“, der es erlaubt, Geräte – und in weiterer Folge den konkreten Nutzer – eindeutig zu individualisieren, ein personenbezogenes Datum darstellt (vgl. *Karg in Simitis/Hornung/Spiecker*, DSGVO Kommentar Art. 4 Z 1 Rz 52 mwN). Diese Überlegung kann aufgrund der Einzigartigkeit der Kennnummern auf den gegenständlichen Fall übertragen werden, zumal – worauf sogleich näher einzugehen ist – diese Kennnummern auch mit weiteren Elementen kombiniert werden können.

Soweit die Beschwerdegegner ins Treffen führen, dass keine „Mittel“ verwendet würden, um die hier gegenständlichen Kennnummern mit der Person des Beschwerdeführers in Verbindung zu bringen, ist ihnen neuerlich entgegenzuhalten, dass die Implementierung von Google Analytics auf www.xyz.at eine Aussonderung iSd ErwGr 26 DSGVO zur Folge hat. Mit anderen Worten: Wer ein Tool verwendet,

welches eine solche Aussonderung gerade erst ermöglicht, kann sich nicht auf den Standpunkt stellen, nach „allgemeinem Ermessen“ keine Mittel zu verwenden, um natürliche Personen identifizierbar zu machen.

Als Zwischenergebnis ist daher festzuhalten, dass die hier gegenständlichen Google Analytics Kennnummern personenbezogene Daten (in Form einer Online-Kennung) gemäß Art. 4 Z 1 DSGVO sein können.

c) Kombination mit weiteren Elementen

Noch deutlicher erkennbar wird die Erfüllung des Tatbestands von Art. 4 Z 1 DSGVO, wenn man berücksichtigt, dass die Kennnummern mit weiteren Elementen kombiniert werden können:

Durch eine Kombination all dieser Elemente – also einzigartige Kennnummern und die weiteren, oben angeführten Informationen wie Browserdaten oder IP-Adresse – ist es nämlich umso wahrscheinlicher, dass der Beschwerdeführer identifiziert werden kann (vgl. erneut ErwGr 30 DSGVO). Der „digitale Fußabdruck“ des Beschwerdeführers wird durch eine solche Kombination noch einzigartiger.

Dabei kann das Vorbringen der Beschwerdegegner rund um die „Anonymisierungsfunktion der IP-Adresse“ dahingestellt bleiben, da die Beschwerdegegner eingeräumt haben, dass diese Funktion (zum beschwerdegegenständlichen Zeitpunkt) nicht korrekt implementiert wurde (vgl. etwa die Stellungnahme der Erstbeschwerdegegnerin vom 18. Juni 2021).

Ebenso kann die Frage, ob eine IP-Adresse isoliert betrachtet ein personenbezogenes Datum ist, dahingestellt bleiben, da diese – wie erwähnt – mit weiteren Elementen (insbesondere der Google Analytics Kennnummer) kombiniert werden kann. In diesem Zusammenhang ist anzumerken, dass die IP-Adresse nach Judikatur des EuGH ein personenbezogenes Datum darstellen kann (vgl. die Urteile des EuGH vom 17. Juni 2021, C-597/19, Rz 102, sowie vom 19. Oktober 2016, C-582/14, Rz 49) und diese ihre Eigenschaft als personenbezogenes Datum nicht bloß deshalb verliert, weil die Mittel zur Identifizierbarkeit bei einem Dritten liegen.

Schließlich weist die Datenschutzbehörde darauf hin, dass es gerade ein wesentlicher Bestandteil des Konzepts von Google Analytics (jedenfalls in der unentgeltlichen Version) ist, auf möglichst vielen Websites implementiert zu werden, um Informationen über Website-Besuchern zu sammeln. Demzufolge wäre es mit dem Grundrecht auf Datenschutz gemäß Art. 8 EU-GRC bzw. § 1 DSG unvereinbar, die Anwendbarkeit der DSGVO auf die mit dem Tool Google Analytics im Zusammenhang stehenden Datenverarbeitungen – bei denen einzelne Website-Besucher anhand der Google Analytics Kennnummer individualisiert werden – auszuschließen.

d) Rückführbarkeit auf den Beschwerdeführer

Unabhängig von den obenstehenden Überlegungen ist aber ohnedies von einer Rückführbarkeit zum „Gesicht“ des Beschwerdeführers – etwa dessen Namen – auszugehen:

Es ist nämlich nicht erforderlich, dass die Beschwerdegegner jeweils alleine einen Personenbezug herstellen können, dass also alle für die Identifizierung erforderlichen Informationen bei diesen sind (vgl. die Urteile des EuGH vom 20. Dezember 2017, C-434/16, Rz 31, sowie vom 19. Oktober 2016, C-582/14, Rz 43). Vielmehr ist ausreichend, dass irgendjemand – mit rechtlich zulässigen Mitteln und vertretbarem Aufwand – diesen Personenbezug herstellen kann (vgl. *Bergauer* in *Jahnel*, DSGVO Kommentar Art. 4 Z 1 Rz 20 mVa *Albrecht/Jožo*, Das neue Datenschutzrecht der EU 58).

Eine derartige Interpretation des Anwendungsbereichs von Art. 4 Z 1 DSGVO ist – neben den angeführten Rechts- und Literaturquellen – aus ErwGr 26 DSGVO ableitbar, wonach bei der Frage der Identifizierbarkeit nicht nur die Mittel des Verantwortlichen (hier: der Erstbeschwerdegegnerin) zu berücksichtigen sind, sondern auch jene „einer anderen Person“ (englische Sprachfassung der Verordnung: „by another person“). Ebenso ergibt sich dies aus dem Gedanken, betroffenen Personen einen möglichst großen Schutz ihrer Daten zu bieten.

So hat der EuGH wiederholt ausgesprochen, dass der Anwendungsbereich der DSGVO „sehr weit“ zu verstehen ist (vgl. etwa die Urteile des EuGH vom 22. Juni 2021, C-439/19, Rz 61; zur insofern vergleichbaren Rechtslage die Urteile vom 20. Dezember 2017, C-434/16, Rz 33, sowie vom 7. Mai 2009, C-553/07, Rz 59).

Nicht übersehen wird, dass nach ErwGr 26 DSGVO auch zu berücksichtigen ist, mit welcher „Wahrscheinlichkeit“ irgendjemand Mittel nutzt, um natürliche Person direkt oder indirekt zu identifizieren. Tatsächlich ist nach Auffassung der Datenschutzbehörde der Begriff „irgendjemand“ – und somit der Anwendungsbereich des Art. 4 Z 1 DSGVO – zwar nicht derart weit zu interpretieren, dass irgendein unbekannter Akteur theoretisch Spezialwissen haben könnte, um einen Personenbezug herzustellen; dies würde nämlich dazu führen, dass beinahe jede Information in den Anwendungsbereich der DSGVO fällt und eine Abgrenzung zu nicht-personenbezogenen Daten schwierig oder gar unmöglich wird.

Entscheidend ist vielmehr, ob mit vertretbarem und zumutbarem Aufwand eine Identifizierbarkeit hergestellt werden kann (vgl. dazu den Bescheid vom 5. Dezember 2018, GZ DSB-D123.270/0009-DSB/2018, wonach personenbezogene Daten nicht – mehr – vorliegen, wenn der Verantwortliche oder ein Dritter nur mit unverhältnismäßigem Aufwand einen Personenbezug herstellen kann).

Im gegenständlichen Fall gibt es aber nun bestimmte Akteure, die ein Spezialwissen besitzen, welches es ermöglicht, im Sinne der obigen Ausführungen einen Bezug zum Beschwerdeführer herstellen und ihn daher zu identifizieren.

Dies ist zunächst der Zweitbeschwerdegegner:

Wie sich aus den Sachverhaltsfeststellungen ergibt, war der Beschwerdeführer im Zeitpunkt des Besuchs der Website www.xyz.at mit seinem Google-Account musteremail123@gmail.com eingeloggt. Der Zweitbeschwerdegegner hat ausgeführt, dass dieser aufgrund des Umstands, dass das Tool Google Analytics auf einer Website implementiert ist, Informationen erhält. Hierzu zählt die Information, dass ein gewisser Google-Account-Nutzer eine gewisse Website besucht hat (vgl. die Stellungnahme vom 9. April 2021, Frage 9).

Dies bedeutet, dass der Zweitbeschwerdegegner zumindest die Information erhalten hat, dass der Nutzer des Google-Accounts musteremail123@gmail.com die Website www.xyz.at besucht hat.

Selbst wenn man also die Auffassung vertritt, dass die oben angeführten Online-Kennungen einem gewissen „Gesicht“ zuordenbar sein müssen, kann eine solche Zuordnung jedenfalls über den Google-Account des Beschwerdeführers erfolgen.

Nicht übersehen werden die weiteren Ausführungen des Zweitbeschwerdegegners, dass für eine solche Zuordnung gewisse Voraussetzungen zu erfüllen seien, wie etwa die Aktivierung von spezifischen Einstellungen im Google-Account (vgl. erneut dessen Stellungnahme vom 9. April 2021, Frage 9).

Wenn jedoch – und dies hat der Beschwerdeführer überzeugend ausgeführt – die Identifizierbarkeit eines Website-Besuchers nur davon abhängt, ob gewisse Willenserklärungen im Konto abgegeben werden, liegen (aus technischer Sicht) alle Möglichkeiten für eine Identifizierbarkeit vor. Bei anderer Betrachtung könnte der Zweitbeschwerdegegner den in den Kontoeinstellungen ausgedrückten Wünschen eines Nutzers nach „Personalisierung“ der erhaltenen Werbeinformationen nicht entsprechen.

In diesem Zusammenhang ist ausdrücklich auf den unmissverständlichen Wortlaut von Art. 4 Z 1 DSGVO hinzuweisen, der an ein Können anknüpft („identifiziert werden kann“) und nicht daran, ob eine Identifizierung letztlich auch vorgenommen wird.

Ebenso ist ausdrücklich auf die in der DSGVO verankerte Rechenschaftspflicht der Erstbeschwerdegegnerin – als Verantwortliche, hierzu weiter unten – hinzuweisen, gemäß Art. 5 Abs. 2 iVm Art. 24 Abs. 1 iVm Art. 28 Abs. 1 DSGVO geeignete technische und organisatorische Maßnahmen einzusetzen, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung (mithilfe eines Auftragsverarbeiters) gemäß der Verordnung erfolgt. Es handelt sich daher um eine Bringschuld.

Hierzu zählt auch der Nachweis, dass eine Verarbeitung gerade nicht der Verordnung unterliegt. Ein solcher wurde – trotz mehrfach eingeräumter Möglichkeiten – nicht erbracht.

Unabhängig vom Zweitbeschwerdegegner sind aber – und dies ist fallbezogen von größerer Relevanz – die US-Behörden zu berücksichtigen:

Wie der Beschwerdeführer ebenso zutreffender Weise ausgeführt hat, nehmen Nachrichtendienste der USA gewisse Online-Kennungen (wie die IP-Adresse oder einzigartige Kennnummern) als Ausgangspunkt für die Überwachung von Einzelpersonen. So kann insbesondere nicht ausgeschlossen werden, dass diese Nachrichtendienste bereits Informationen gesammelt haben, mit deren Hilfe die hier übertragenen Daten auf die Person des Beschwerdeführers rückführbar sind.

Der Umstand, dass es sich hierbei nicht bloß um eine „theoretische Gefahr“ handelt, zeigt sich am Urteil des EuGH vom 16. Juli 2020, C-311/18, der aufgrund der Unvereinbarkeit solcher Methoden und Zugriffsmöglichkeiten der US-Behörden mit dem Grundrecht auf Datenschutz gemäß Art. 8 EU-GRC letztlich auch den EU-US-Angemessenheitsbeschluss („Privacy Shield“) für ungültig erklärt hat.

Insbesondere zeigt sich dies am – in den Sachverhaltsfeststellungen angeführten – Transparenzbericht des Zweitbeschwerdegegners, der belegt, dass es zu Datenanfragen von US-Behörden an den Zweitbeschwerdegegner kommt. Dabei können Metadaten und Inhaltsdaten vom Zweitbeschwerdegegner angefordert werden.

Zwar wird nicht verkannt, dass es der Erstbeschwerdegegnerin freilich nicht möglich ist, zu überprüfen, ob es zu derartigen Zugriffen von US-Behörden im Einzelfall – also pro Website-Besucher – kommt und welche Informationen US-Behörden bereits besitzen; umgekehrt kann dieser Umstand aber betroffenen Personen, wie dem Beschwerdeführer, nicht zur Last gelegt werden. So war es letztlich die Erstbeschwerdegegnerin als (damaliger) Websitebetreiberin, die – trotz Veröffentlichung des genannten Urteils des EuGH vom 16. Juli 2020 – das Tool Google Analytics weiterhin eingesetzt hat.

Als weiteres Zwischenergebnis ist daher festzuhalten, dass es sich bei den in den Sachverhaltsfeststellungen unter C.9. angeführten Informationen (jedenfalls in Kombination) um personenbezogene Daten gemäß Art. 4 Z 1 DSGVO handelt.

e) Rollenverteilung

Wie bereits ausgeführt, hat die Erstbeschwerdegegnerin als Website-Betreiberin zum beschwerdegegenständlichen Zeitpunkt die Entscheidung getroffen, das Tool „Google Analytics“ auf der Website www.xyz.at zu implementieren. Konkret hat sie einen JavaScript Code („tag“), der seitens des Zweitbeschwerdegegners zur Verfügung gestellt wird, im Quelltext ihrer Website eingefügt, wodurch dieser JavaScript Code beim Besuch der Website im Browser des Beschwerdeführers ausgeführt wurde. Die Erstbeschwerdegegnerin hat diesbezüglich ausgeführt, dass das genannte Tool zum Zwecke von statistischen Auswertungen über das Verhalten der Websitebesucher eingesetzt wird (vgl. Stellungnahme vom 16. Dezember 2020, Frage 2).

Dadurch hat die Erstbeschwerdegegnerin über „Zwecke und Mittel“ der mit dem Tool in Verbindung stehenden Datenverarbeitung entschieden, weshalb diese (jedenfalls) als Verantwortliche iSd Art. 4 Z 7 DSGVO anzusehen ist.

Was den Zweitbeschwerdegegner betrifft, ist festzuhalten, dass sich der hier relevante Beschwerdegegenstand (nur) auf die Datenübermittlung an den Zweitbeschwerdegegner in die USA bezieht. Eine mögliche weitere Datenverarbeitung der in den Sachverhaltsfeststellungen unter C.9. angeführten Informationen (durch Google Ireland Limited oder dem Zweitbeschwerdegegner) ist nicht Beschwerdegegenstand und wurde somit auch nicht näher in diese Richtung ermittelt.

Was nun die Datenverarbeitungen im Zusammenhang mit dem Tool Google Analytics betrifft, ist festzuhalten, dass der Zweitbeschwerdegegner dieses lediglich zur Verfügung stellt und auch keinen Einfluss darauf hat, ob überhaupt und inwiefern die Erstbeschwerdegegnerin von den Toolfunktionen Gebrauch macht und welche konkreten Einstellungen sie wählt.

Soweit der Zweitbeschwerdegegner daher Google Analytics (als Dienstleistung) nur bereitstellt, nimmt dieser keinen Einfluss auf „Zwecke und Mittel“ der Datenverarbeitung und ist daher iSd Art. 4 Z 8 DSGVO fallbezogen als Auftragsverarbeiter zu qualifizieren.

Diese Überlegungen erfolgen unbeschadet eines weiteren amtswegigen Prüfverfahrens gemäß Art. 58 Abs. 1 lit. b DSGVO und unbeschadet der datenschutzrechtlichen Rolle des Zweitbeschwerdegegners im Hinblick auf eine mögliche weitere Datenverarbeitung.

D.3. Spruchpunkt 2. b)

a) Anwendungsbereich von Kapitel V DSGVO

Zunächst ist zu überprüfen, ob die Erstbeschwerdegegnerin den in Kapitel V der Verordnung normierten Pflichten unterliegt.

Gemäß Art. 44 DSGVO ist jedwede „[...] Übermittlung personenbezogener Daten, die bereits verarbeitet werden oder nach ihrer Übermittlung an ein Drittland oder eine internationale Organisation verarbeitet werden sollen, [...] nur zulässig, wenn der Verantwortliche und der Auftragsverarbeiter die in diesem Kapitel niedergelegten Bedingungen einhalten und auch die sonstigen Bestimmungen dieser Verordnung eingehalten werden; dies gilt auch für die etwaige Weiterübermittlung personenbezogener Daten aus dem betreffenden Drittland oder der betreffenden internationalen Organisation an ein anderes Drittland oder eine andere internationale Organisation. Alle Bestimmungen dieses Kapitels sind anzuwenden, um sicherzustellen, dass das durch diese Verordnung gewährleistete Schutzniveau für natürliche Personen nicht untergraben wird.“

In den „Leitlinien 5/2021 zum Verhältnis zwischen dem Anwendungsbereich von Art. 3 und den Vorgaben für den Internationalen Datenverkehr gemäß Kapitel V DSGVO“ (aktuell noch in öffentlicher

Konsultation), hat der EDSA drei kumulative Voraussetzungen identifiziert, wann eine „Übermittlung an ein Drittland oder eine internationale Organisation“ iSd Art. 44 DSGVO vorliegt (ebd. Rz 7):

- der für die Verarbeitung Verantwortliche oder ein Auftragsverarbeiter unterliegt bei der betreffenden Verarbeitung der DSGVO;
- dieser für die Verarbeitung Verantwortliche oder Auftragsverarbeiter („Datenexporteur“) legt durch Übermittlung oder auf andere Weise personenbezogene Daten, die Gegenstand dieser Verarbeitung sind, einem anderen für die Verarbeitung Verantwortlichen, einem gemeinsam Verantwortlichen oder einem Auftragsverarbeiter, offen („Datenimporteur“);
- der Datenimporteur befindet sich in einem Drittland oder ist eine internationale Organisation, unabhängig davon, ob dieser Datenimporteur in Bezug auf die betreffende Verarbeitung gemäß Art. 3 der DSGVO unterliegt oder nicht.

Die Erstbeschwerdegegnerin hat ihren Sitz in Österreich und war im beschwerdegegenständlichen Zeitpunkt für den Betrieb der Website www.xyz.at datenschutzrechtliche Verantwortliche. Darüber hinaus hat die Erstbeschwerdegegnerin (als Datenexporteurin) personenbezogene Daten des Beschwerdeführers dadurch offengelegt, dass sie proaktiv das Tool Google Analytics auf ihrer Website www.xyz.at implementiert hat und als direkte Folge dieser Implementierung u.a. eine Datenübermittlung an den Zweitbeschwerdegegner (in die USA) stattfand. Schließlich hat der Zweitbeschwerdegegner in seiner Eigenschaft als Auftragsverarbeiter (und Datenimporteur) seinen Sitz in den USA.

Da alle in den Leitlinien des EDSA dargelegten Voraussetzungen erfüllt sind, unterliegt die Erstbeschwerdegegnerin als Datenexporteurin den Bestimmungen des Kapitels V der Verordnung.

b) Regelwerk von Kapitel V DSGVO

In weiterer Folge ist zu überprüfen, ob die Datenübermittlung in Einklang mit den Vorgaben von Kapitel V DSGVO in die USA stattgefunden hat.

Kapitel V der Verordnung sieht drei Instrumente vor, um das von Art. 44 DSGVO geforderte angemessene Schutzniveau für Datenübermittlungen an ein Drittland oder eine internationale Organisation sicherzustellen:

- Angemessenheitsbeschluss (Art. 45 DSGVO);
- Geeignete Garantien (Art. 46 DSGVO);
- Ausnahmen für bestimmte Fälle (Art. 49 DSGVO).

c) Angemessenheitsbeschluss

Der EuGH hat ausgesprochen, dass der EU-US Angemessenheitsbeschluss („Privacy Shield“) – ohne Aufrechterhaltung seiner Wirkung – ungültig ist (vgl. das Urteil vom 16. Juli 2020, C-311/18 Rz 201 f).

Die gegenständliche Datenübermittlung findet daher keine Deckung in Art. 45 DSGVO.

d) Geeignete Garantien

Wie sich aus den Sachverhaltsfeststellungen ergibt, haben die Beschwerdegegner am 12. August 2020 Standarddatenschutzklauseln (in Folge: SDK) gemäß Art. 46 Abs. 2 lit. c DSGVO für die Übermittlung personenbezogener Daten in die USA abgeschlossen („Google Ads Data Processing Terms: Model Contract Clauses, Standard Contractual Clauses for Processors“). Konkret handelte es sich zum beschwerdegegenständlichen Zeitpunkt um jene Klauseln in der Fassung des Durchführungsbeschlusses der Europäischen Kommission 2010/87/EU vom 5. Februar 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates, ABl. L 2010/39, S. 5.

Im erwähnten Urteil vom 16. Juli 2020 hat der EuGH zwar ausgeführt, dass SDK als Instrument für den Internationalen Datenverkehr dem Grunde nach nicht zu beanstanden sind, allerdings hat der EuGH auch darauf hingewiesen, dass SDK ihrer Natur nach ein Vertrag sind und demnach Behörden aus einem Drittstaat nicht binden können:

„Demnach gibt es zwar Situationen, in denen der Empfänger einer solchen Übermittlung in Anbetracht der Rechtslage und der Praxis im betreffenden Drittland den erforderlichen Datenschutz allein auf der Grundlage der Standarddatenschutzklauseln garantieren kann, aber auch Situationen, in denen die in diesen Klauseln enthaltenen Regelungen möglicherweise kein ausreichendes Mittel darstellen, um in der Praxis den effektiven Schutz der in das betreffende Drittland übermittelten personenbezogenen Daten zu gewährleisten. So verhält es sich etwa, wenn das Recht dieses Drittlands dessen Behörden Eingriffe in die Rechte der betroffenen Personen bezüglich dieser Daten erlaubt“ (ebd. Rz 126).

Eine nähere Analyse der Rechtslage der USA (als Drittland) kann an dieser Stelle jedoch unterbleiben, da sich der EuGH mit dieser bereits im angeführten Urteil vom 16. Juli 2020 auseinandergesetzt hat. Dabei ist er zu dem Ergebnis gekommen, dass der EU-US Angemessenheitsbeschluss aufgrund des einschlägigen Rechts der USA und der Durchführung von behördlichen Überwachungsprogrammen – u.a. gestützt auf Section 702 des FISA und die E.O. 12333 in Verbindung mit der PPD-28 – kein angemessenes Schutzniveau für natürliche Personen gewährleistet (ebd. Rz 180 ff).

Diese Überlegungen können auf den gegenständlichen Fall übertragen werden. So ist offenkundig, dass der Zweitbeschwerdegegner als Anbieter elektronischer Kommunikationsdienste im Sinne von 50 U.S.Code § 1881(b)(4) zu qualifizieren ist und somit der Überwachung durch US-Nachrichtendienste gemäß 50 U.S.Code § 1881a („FISA 702“) unterliegt. Demnach hat der Zweitbeschwerdegegner die Verpflichtung, den US-Behörden gemäß 50 U.S. Code § 1881a personenbezogene Daten zur Verfügung zu stellen.

Wie sich aus dem Transparenzbericht („Transparency Report“) des Zweitbeschwerdegegners ergibt, werden auch regelmäßig derartige Anfragen von US-Behörden an diesen gestellt (vgl. <https://transparencyreport.google.com/user-data/us-national-security?hl=en>, abgefragt am 22. Dezember 2021).

Wenn nun aber bereits der EU-US Angemessenheitsbeschluss aufgrund der Rechtslage in den USA für ungültig erklärt wurde, so kann fallbezogen nicht davon ausgegangen werden, dass der (bloße) Abschluss von SDK ein angemessenes Schutzniveau nach Art. 44 DSGVO für die gegenständliche Datenübermittlung gewährleistet.

Vor diesem Hintergrund hat der EuGH im angeführten Urteil vom 16. Juli 2020 auch festgehalten, dass *„[...] Standarddatenschutzklauseln ihrer Natur nach keine Garantien bieten können, die über die vertragliche Verpflichtung, für die Einhaltung des unionsrechtlich verlangten Schutzniveaus zu sorgen, hinausgehen [...]“* und es *„[...] je nach der in einem bestimmten Drittland gegebenen Lage erforderlich sein [kann], dass der Verantwortliche zusätzliche Maßnahmen ergreift, um die Einhaltung dieses Schutzniveaus zu gewährleisten“* (ebd. Rz 133).

Die gegenständliche Datenübermittlung kann daher nicht allein auf die zwischen den Beschwerdegegnern abgeschlossenen Standarddatenschutzklauseln gemäß Art. 46 Abs. 2 lit. c DSGVO gestützt werden.

e) Allgemeines zu „zusätzliche Maßnahmen“

In seinen „Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten“ hat der EDSA festgehalten, dass für den Fall, dass das Recht des Drittlands sich auf die Wirksamkeit von geeigneten Garantien (wie etwa SDK) auswirkt, der Datenexporteur die Datenübermittlung entweder auszusetzen oder zusätzliche Maßnahmen („supplementary measures“) zu implementieren hat (ebd. Rz 28 ff sowie Rz 52).

Solche „zusätzliche Maßnahmen“ im Sinne des Urteils des EuGH vom 16. Juli 2020 können laut den Empfehlungen des EDSA vertraglicher, technischer oder organisatorischer Art sein (ebd. Rz 47):

Im Hinblick auf vertragliche Maßnahmen wird festgehalten, dass *diese „[...] die Garantien, die das Übermittlungsinstrument und die einschlägigen Rechtsvorschriften im Drittland bieten, ergänzen und verstärken, soweit die Garantien, unter Berücksichtigung sämtlicher Umstände der Übermittlung, nicht alle Voraussetzungen erfüllen, die erforderlich sind, um ein Schutzniveau zu gewährleisten, das dem in der EU im Wesentlichen gleichwertig ist. Da die vertraglichen Maßnahmen ihrer Art nach die Behörden des Drittlands im Allgemeinen nicht binden können, wenn diese nicht selbst Vertragspartei sind, müssen sie mit anderen technischen und organisatorischen Maßnahmen kombiniert werden, um das erforderliche Datenschutzniveau zu gewährleisten. Nur weil man eine oder mehrere dieser*

Maßnahmen ausgewählt und angewendet hat, bedeutet das noch nicht unbedingt, dass systematisch sichergestellt ist, dass die vorgesehene Übermittlung den unionsrechtlichen Anforderungen (Gewährleistung eines im Wesentlichen gleichwertigen Schutzniveaus) genügt“ (ebd. Rz 93).

Zu organisatorischen Maßnahmen wird ausgeführt, dass es sich „[...] um interne Strategien, Organisationsmethoden und Standards handeln [kann], die die Verantwortlichen und Auftragsverarbeiter bei sich selbst anwenden und den Datenimporteuren in Drittländern auferlegen könnten. [...] Je nach den besonderen Umständen der Übermittlung und der durchgeführten Beurteilung der Rechtslage im Drittland sind organisatorische Maßnahmen zur Ergänzung der vertraglichen und/oder technischen Maßnahmen erforderlich, um sicherzustellen, dass der Schutz der personenbezogenen Daten dem in der EU gewährleisteten Schutzniveau im Wesentlichen gleichwertig ist (ebd. Rz 122).

Zu technischen Maßnahmen wird ausgeführt, dass durch diese sichergestellt werden soll, dass „[...] der Zugang der Behörden in Drittländern zu den übermittelten Daten die Effektivität der in Artikel 46 DSGVO aufgeführten geeigneten Garantien nicht untergräbt. Selbst wenn der behördliche Zugriff mit dem Recht im Land des Datenimporteurs in Einklang steht, sind diese Maßnahmen in Betracht zu ziehen, wenn der behördliche Zugriff über das hinausgeht, was in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt. Diese Maßnahmen zielen darauf ab, potenziell rechtsverletzende Zugriffe auszuschließen, indem sie die Behörden daran hindern, betroffene Personen zu identifizieren, Informationen über sie zu erschließen, sie in anderen Kontexten zu ermitteln oder die übermittelten Daten mit anderen Datensätzen im Behördenbesitz zu verknüpfen, die unter anderem Daten über Online-Kennungen der Geräte, Anwendungen, Tools und Protokolle enthalten, die die betroffenen Personen in anderen Zusammenhängen benutzt haben (ebd. Rz 74).

Schließlich hat der EDSA festgehalten, dass derartige „zusätzliche Maßnahmen“ nur dann als effektiv im Sinne des Urteils vom 16. Juli 2020 zu betrachten sind, „[...] sofern und soweit die Maßnahme genau die Rechtsschutzlücken schließt, die der Datenexporteur bei seiner Prüfung der Rechtslage im Drittland festgestellt hat. Sollte es dem Datenexporteur letztendlich nicht möglich sein, ein im Wesentlichen gleichwertiges Schutzniveau zu erzielen, darf er die personenbezogenen Daten nicht übermitteln“ (ebd. Rz 70).

Umgelegt auf den gegenständlichen Fall bedeutet dies, dass zu untersuchen ist, ob die „zusätzlich getroffenen Maßnahmen“ des Zweitbeschwerdegegners die im Rahmen des EuGH-Urteils vom 20. Juni 2020 aufgezeigten Rechtsschutzlücken – also die Zugriffs- und Überwachungsmöglichkeiten von US-Nachrichtendiensten – schließen.

f) „Zusätzliche Maßnahmen“ des Zweitbeschwerdegegners

Der Zweitbeschwerdegegner hat nun zusätzlich zum Abschluss der SDK diverse Maßnahmen implementiert (vgl. dessen Stellungnahme vom 9. April 2021, Frage 28).

In Bezug auf die dargelegten vertraglichen und organisatorischen Maßnahmen ist nicht erkennbar, inwiefern eine Benachrichtigung der betroffenen Person über Datenanfragen (sollte dies im Einzelfall überhaupt zulässig sein), die Veröffentlichung eines Transparenzberichts oder eine „Richtlinie für den Umgang mit Regierungsanfragen“ effektiv im Sinne der obigen Überlegungen sind. Ebenso ist unklar, inwiefern die „sorgfältige Prüfung einer jeder Datenzugriffsanfrage“ eine effektive Maßnahme darstellt, da der EuGH im genannten Urteil vom 20. Juni 2020 ausgesprochen hat, dass zulässige (also gemäß dem Recht der USA legale) Anfragen von US-Nachrichtendiensten nicht mit dem Grundrecht auf Datenschutz gemäß Art. 8 EU-GRC vereinbar sind.

Sofern die technischen Maßnahmen betroffen sind, ist ebenso nicht erkennbar – und wurde seitens der Beschwerdegegner auch nicht nachvollziehbar erklärt –, inwiefern der Schutz der Kommunikation zwischen Google-Diensten, der Schutz von Daten im Transit zwischen Rechenzentren, der Schutz der Kommunikation zwischen Nutzern und Websites oder eine „On-Site-Security“ die Zugriffsmöglichkeiten von US-Nachrichtendiensten auf der Grundlage des US-Rechts tatsächlich verhindern oder einschränken.

Sofern der Zweitbeschwerdegegner in Folge auf Verschlüsselungstechnologien – etwa auf die Verschlüsselung von „Daten im Ruhezustand“ in den Datenzentren – verweist, sind ihm erneut die Empfehlungen 01/2020 des EDSA entgegenzuhalten. Dort wird nämlich ausgeführt, dass ein Datenimporteur (wie der Zweitbeschwerdegegner), der 50 U.S. Code § 1881a („FISA 702“) unterliegt, hinsichtlich der importierten Daten, die sich in seinem Besitz oder Gewahrsam oder unter seiner Kontrolle befinden, eine direkte Verpflichtung hat, den Zugriff darauf zu gewähren oder diese herauszugeben. Diese Verpflichtung kann sich ausdrücklich auch auf die kryptografischen Schlüssel erstrecken, ohne die die Daten nicht lesbar sind (ebd. Rz 76).

Solange der Zweitbeschwerdegegner sohin selbst die Möglichkeit hat, auf Daten im Klartext zuzugreifen, können die ins Treffen geführten technischen Maßnahmen nicht als effektiv im Sinne der obigen Überlegungen betrachtet werden.

Der Zweitbeschwerdegegner führt als weitere technische Maßnahme ins Treffen, dass soweit „[...] Google Analytics Daten zur Messung durch Website-Besitzer personenbezogene Daten sind, [...] sie als pseudonym betrachtet werden“ müssten (vgl. dessen Stellungnahme vom 9. April 2021, S. 26).

Dem ist jedoch die überzeugende Ansicht der Deutschen Datenschutzkonferenz entgegenzuhalten, wonach „[...] die Tatsache, dass die Nutzer etwa über IDs oder Kennungen bestimmbar gemacht werden, keine Pseudonymisierungsmaßnahme i. S. d. DSGVO darstellt. Zudem handelt es sich nicht

um geeignete Garantien zur Einhaltung der Datenschutzgrundsätze oder zur Absicherung der Rechte betroffener Personen, wenn zur (Wieder-)Erkennung der Nutzer IP-Adressen, Cookie-IDs, Werbe-IDs, Unique-User-IDs oder andere Identifikatoren zum Einsatz kommen. Denn, anders als in Fällen, in denen Daten pseudonymisiert werden, um die identifizierenden Daten zu verschleiern oder zu löschen, so dass die betroffenen Personen nicht mehr adressiert werden können, werden IDs oder Kennungen dazu genutzt, die einzelnen Individuen unterscheidbar und adressierbar zu machen. Eine Schutzwirkung stellt sich folglich nicht ein. Es handelt sich daher nicht um Pseudonymisierungen i. S. d. ErwGr 28, die die Risiken für die betroffenen Personen senken und die Verantwortlichen und die Auftragsverarbeiter bei der Einhaltung ihrer Datenschutzpflichten unterstützen“ (vgl. die Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien aus März 2019, S. 15).

Darüber hinaus ist dem Vorbringen des Zweitbeschwerdegegners auch deshalb nicht zu folgen, weil die Google Analytics Kennung – wie oben ausgeführt – ohnedies mit weiteren Elementen kombiniert und sogar mit einem dem Beschwerdeführer unstrittig zuzurechnenden Google Account in Verbindung gebracht werden kann.

Die angesprochene „Anonymisierungsfunktion der IP-Adresse“ ist fallbezogen nicht von Relevanz, da diese – wie ebenfalls oben ausgeführt – nicht korrekt implementiert wurde. Abgesehen davon ist die IP-Adresse ohnedies nur eines von vielen „Puzzleteilen“ des digitalen Fußabdrucks des Beschwerdeführers.

Als weiteres Zwischenergebnis ist daher festzuhalten, dass die gegenständlichen „zusätzlichen Maßnahmen“ nicht effektiv sind, da diese die im Rahmen des Urteils des EuGH vom 20. Juni 2020 aufgezeigten Rechtsschutzlücken – also die Zugriffs- und Überwachungsmöglichkeiten von US-Nachrichtendiensten – nicht schließen.

Die gegenständliche Datenübermittlung findet somit auch keine Deckung in Art. 46 DSGVO.

D.4. Spruchpunkt 2. c)

a) Zu Art. 49 DSGVO

Laut eigenen Angaben der Erstbeschwerdegegnerin war die Ausnahmeregelung gemäß Art. 49 DSGVO für die gegenständliche Datenübermittlung nicht von Relevanz (vgl. die Stellungnahme vom 16. Dezember 2020).

Eine Einwilligung gemäß Art. 49 Abs. 1 lit. a DSGVO wurde nicht eingeholt. Für die Datenschutzbehörde ist auch nicht erkennbar, inwiefern ein sonstiger Tatbestand von Art. 49 DSGVO erfüllt sein soll.

Die gegenständliche Datenübermittlung kann daher auch nicht auf Art. 49 DSGVO gestützt werden.

b) Ergebnis

Da für die gegenständliche Datenübermittlung der Erstbeschwerdegegnerin an den Zweitbeschwerdegegner (in den USA) kein angemessenes Schutzniveau durch ein Instrument von Kapitel V der Verordnung gewährleistet wurde, liegt eine Verletzung von Art. 44 DSGVO vor.

Die Erstbeschwerdegegnerin war (jedenfalls) zum beschwerderelevanten Zeitpunkt – also dem 14. August 2020 – für den Betrieb der Website www.xyz.at verantwortlich. Der hier relevante datenschutzrechtliche Verstoß gegen Art. 44 DSGVO ist daher der Erstbeschwerdegegnerin zuzurechnen.

Es war daher spruchgemäß zu entscheiden.

D.5. Zu den Abhilfebefugnissen

Nach Auffassung der Datenschutzbehörde kann das Tool Google Analytics (jedenfalls in der Version vom 14. August 2020) somit nicht in Einklang mit den Vorgaben von Kapitel V DSGVO genutzt werden.

Da die Zuständigkeit für den Betrieb der Website www.xyz.at im Laufe des Beschwerdeverfahrens (allerdings erst nach dem 14. August 2020) auf die XYZ123 GmbH mit Sitz in Musterstadt übergegangen und Google Analytics im Entscheidungszeitpunkt weiterhin implementiert ist, wird die Datenschutzbehörde hinsichtlich der (möglichen) Inanspruchnahme der Abhilfebefugnisse gemäß Art. 58 Abs. 2 DSGVO den Fall an die zuständige deutsche Aufsichtsbehörde herantragen.

D.6. Spruchpunkt 3

Zu überprüfen ist, ob auch der Zweitbeschwerdegegner (als Datenimporteur) den in Kapitel V der Verordnung normierten Pflichten unterliegt.

Ausgehend von den bereits oben angeführten Leitlinien 5/2021 des EDSA ist erneut festzuhalten, dass eine Übermittlung an ein Drittland oder eine internationale Organisation“ iSd Art. 44 DSGVO nur dann vorliegt, wenn u.a. der für die Verarbeitung Verantwortliche oder Auftragsverarbeiter (Datenexporteur) durch Übermittlung oder auf andere Weise personenbezogene Daten, die Gegenstand dieser Verarbeitung sind, einem anderen für die Verarbeitung Verantwortlichen, einem gemeinsam Verantwortlichen oder einem Auftragsverarbeiter (Datenimporteur), offenlegt.

Diese Voraussetzung trifft im vorliegenden Fall nicht auf den Zweitbeschwerdegegner zu, da dieser (als Datenimporteur) die personenbezogenen Daten des Beschwerdeführers nicht offenlegt, sondern sie

(nur) erhält. Mit anderen Worten: Die Vorgaben von Kapitel V DSGVO sind vom Datenexporteur, nicht jedoch vom Datenimporteur einzuhalten.

Nicht übersehen wird die Argumentation des Beschwerdeführers, dass eine Datenübermittlung notwendigerweise einen Empfänger voraussetzt und dass der Zweitbeschwerdegegner (jedenfalls aus technischer Sicht) Teil der Datenübermittlung ist. Dem ist jedoch entgegenzuhalten, dass sich die datenschutzrechtliche Verantwortung bei einem Verarbeitungsvorgang (aus rechtlicher Sicht) trotzdem „teilen“ lässt, es also je nach der Phase des Verarbeitungsvorgangs einen unterschiedlichen Grad der Verantwortung geben kann (vgl. die Leitlinien 7/2020 des EDSA zum Konzept von Verantwortlichen und Auftragsverarbeitern, Rz 63 ff mwN).

Eine Verletzung von Art. 44 DSGVO durch den Zweitbeschwerdegegner liegt nach Auffassung der Datenschutzbehörde daher nicht vor.

Insgesamt war daher spruchgemäß zu entscheiden.

Abschließend ist darauf hinzuweisen, dass zur Frage der (möglichen) Verletzung von Art. 5 ff iVm Art. 28 Abs. 3 lit. a und Art. 29 DSGVO durch den Zweitbeschwerdegegner mit einem weiteren Bescheid abgesprochen wird.