



Republik Österreich  
Datenschutz  
behörde

E-Mail: [dsb@dsb.gv.at](mailto:dsb@dsb.gv.at)

Barichgasse 40-42  
A-1030 Wien  
Tel.: +43-1-52152 302565

GZ: [REDACTED]  
[REDACTED]

Sachbearbeiter: [REDACTED]

[REDACTED]

zH noyb – European Center for Digital Rights

Goldschlagstraße 172/4/3/2  
1140 Wien

Datenschutzbeschwerde (Art. 77 Abs. 1 DSGVO)

[REDACTED], vertreten durch NOYB/1. [REDACTED] und 2. Google  
LLC

E-Mail [legal@noyb.eu](mailto:legal@noyb.eu)

## TEILBESCHEID

### SPRUCH

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

1. Der Bescheid der Datenschutzbehörde vom 2. Oktober 2020, [REDACTED], 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 [REDACTED] zumindest am 11. 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-Nachrichtendienste 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, Z 8 und Z 23 lit. b, Art. 5, Art. 44, Art. 46 Abs. 1 und Abs. 2 lit. c, Art. 51 Abs. 1, Art. 56 Abs. 1, Art. 57 Abs. 1 lit. d und lit. f, Art. 60 Abs. 7 und Abs. 8, 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 11. August 2020, um 1:46:00 Uhr, die Website der Erstbeschwerdegegnerin unter [REDACTED] besucht. Während des Besuchs sei er in seinem Google-Konto eingeloggt gewesen, welches mit der E-Mail-Adresse des Beschwerdeführers 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-Nachrichtendienste 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 22. Dezember 2020 brachte die Erstbeschwerdegegnerin zusammengefasst Folgendes vor:

Der Programmcode für das Tool Google Analytics sei auf [REDACTED] eingebettet worden. Ohne Einwilligung werde der Code vom Webserver aber nicht ausgespielt. Die Erstbeschwerdegegnerin sei nur in Österreich ansässig und habe keine weiteren Niederlassungen in anderen Mitgliedstaaten. Sie betreibe folgende europäische Versionen der Website, auf denen das Tool ebenfalls in gleicher Form

eingebunden sei: [REDACTED], [REDACTED], [REDACTED], [REDACTED] und [REDACTED].

Das Tool werde eingesetzt, um allgemeine statistische Auswertungen über das Verhalten der Websitebesucher zu ermöglichen. Das Tool erlaube allerdings nicht, den Content bzw. Suchanfragen 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“). Die Funktion „anonymizeIP“ sei auf „true“ gestellt worden. Damit sei eine Anonymisierung vor Speicherung der Daten gewährleistet. Der Code für das gegenständliche Tool sei derzeit weiterhin auf den Websites vorhanden.

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 C-311/18 nicht einschlägig. 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 beigefügt.

A.3. Mit Stellungnahme vom 12. Februar 2021 brachte der Beschwerdeführer zusammengefasst Folgendes vor:

Die zuerst verarbeitete IP-Adresse würde – wenn überhaupt – 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. Sofern die Erstbeschwerdegegnerin der Überzeugung sei, dass keine personenbezogenen Daten verarbeitet würden, sei etwa der Abschluss von Auftragsverarbeitungsbedingungen widersinnig. Der Stellungnahme waren mehrere Beilagen beigefügt. Es werde die Feststellung beantragt, dass die gegenständlichen Datenübermittlungen unzulässig iSd Art. 44 ff DSGVO waren.

A.4. Die Datenschutzbehörde forderte den Zweitbeschwerdegegner mit Erledigung vom 3. Mai 2021 wie folgt auf (Formatierung nicht 1:1 wiedergegeben):

**„Betrifft: I. Datenschutzbeschwerde gemäß Art. 77 Abs. 1 DSGVO gegen Google LLC; II. Zum Fragebogen vom 9. April 2021**

**I. Datenschutzbeschwerde gemäß Art. 77 Abs. 1 DSGVO gegen Google LLC**

Im Anhang finden Sie eine Datenschutzbeschwerde vom 18. August 2020 gemäß Art. 77 Abs. 1 DSGVO von MB (Beschwerdeführer), vertreten durch NOYB, eine Organisation gemäß Art. 80 Abs. 1 DSGVO, gegen 1. [REDACTED] (Erstbeschwerdegegner) und 2. **Google LLC** (Zweitbeschwerdegegner). Darüber hinaus wird eine Stellungnahme des Erstbeschwerdegegners vom 16. Dezember 2020 übermittelt.

Beschwerdegegenstand ist der Einsatz des Tools Google Analytics durch den Erstbeschwerdegegner auf seiner Website. Google LLC wird ausdrücklich als Zweitbeschwerdegegner genannt. Es wird eine Verletzung der Vorgaben für den internationalen Datenverkehr (Kapitel 5 DSGVO) behauptet.

Ihnen wird die Möglichkeit gegeben, zu dieser Beschwerde innerhalb einer Frist von drei Wochen ab Erhalt dieses Schreibens eine Stellungnahme abzugeben.

**II. Zum Fragebogen vom 9. April 2021**

Google LLC hat in einem parallel anhängigen Beschwerdeverfahren zur Geschäftszahl DSB-D155.027 bereits einen Fragebogen der Datenschutzbehörde zum Thema Google Analytics ausgefüllt und mit Schreiben vom 9. April 2021 entsprechende Antworten an die Datenschutzbehörde übermittelt.

Festgehalten wird, dass die Stellungnahme von Google vom 9. April 2021 derart formuliert ist, dass die Ausführungen auch auf das hier relevante Beschwerdeverfahren gegen [REDACTED] übertragbar sind. Folglich plant die Datenschutzbehörde, den im gegenständlichen Verfahren Beteiligten Parteiengehör zum Schreiben vom 9. April 2021 von Google LLC zu gewähren.

Sollten Sie gegen diese Vorgehensweise Einwände haben, werden Sie ersucht, diese innerhalb einer Frist von drei Wochen ab Erhalt dieses Schreibens mitzuteilen.

Bitte geben Sie bei Ihren Eingaben an die Datenschutzbehörde die Geschäftszahl DSB-D155.026 an.“

A.5. Mit Stellungnahme vom 28. Mai 2021 brachte die Erstbeschwerdegegnerin zusammengefasst Folgendes vor:

Der verfahrensgegenständliche Programmcode für das Tool Google Analytics sei mit 25. Mai 2021 entfernt worden. Die Nutzung von Google Analytics auf der Website [REDACTED] sei damit eingestellt worden. Ein Vorgehen nach § 24 Abs. 6 DSG (formlose Einstellung) werde angeregt.

A.6. Mit Stellungnahme vom 8. Juni 2021 brachte der Beschwerdeführer zusammengefasst Folgendes vor:

Es handle sich um einen in der Vergangenheit gelegenen, in sich abgeschlossenen Sachverhalt und die Entfernung des Programmcodes ändere nichts an der Beschwer des Beschwerdeführers. Die gegenständlichen Daten seien bereits unter Verletzung der Art. 44 ff DSGVO übermittelt worden. Eine entsprechende Feststellung werde beantragt.

A.7. Mit Erledigung vom 25. Juni 2021 übermittelte die Datenschutzbehörde dem Beschwerdeführer und der Erstbeschwerdegegnerin die zuvor erwähnte Stellungnahme des Zweitbeschwerdegegners vom 9. April 2021.

A.8. Mit Stellungnahme vom 6. August 2021 brachte die Erstbeschwerdegegnerin zusammengefasst Folgendes vor:

Sie habe die kostenlose Version von Google Analytics verwendet. Dabei habe sie den Nutzungsbedingungen als auch den SCC zugestimmt. Die Datenaustauscheinstellung sei nicht aktiviert worden. Auch Google Signals sei nicht eingesetzt worden. Man habe sich in Verbindung mit dem Einsatz von Google Analytics nicht auf die Ausnahmeregelung nach Art. 49 Abs. 1 DSGVO gestützt.

A.9. Mit Stellungnahme vom 13. August 2021 brachte der Beschwerdeführer zusammengefasst Folgendes vor:

Man verweise auf die Stellungnahme vom 5. Mai 2021 zum Parallelverfahren zur GZ: DSB-D155.027. Wie auch im Parallelverfahren könne man anhand der übermittelten HAR-Datei erkennen, dass personenbezogene Daten des Beschwerdeführers verarbeitet worden seien und eine Übermittlung der Daten in die USA an Google LLC stattgefunden habe.

A.10. Mit Stellungnahme vom 23. August 2021 brachte die Erstbeschwerdegegnerin zusammengefasst Folgendes vor:

Die Erstbeschwerdegegnerin sei Betreiberin des Vergleichsportals [REDACTED]. Sie betreibe [REDACTED] in den folgenden Sprachversionen: [REDACTED] und [REDACTED].

A.11. Mit Stellungnahme vom 2. November 2021 brachte der Zweitbeschwerdegegner zusammengefasst Folgendes vor:

Die beschwerdegegenständliche IP-Adresse und die Cookie-Daten seien keine personenbezogenen Daten. Es sei die IP-Anonymisierungsfunktion aktiviert gewesen. Die Daten seien dem Beschwerdeführer auch nicht zuordenbar. Der Beschwerdeführer habe nicht dargelegt, welche IP-Adresse das mit dem Internet verbundene Gerät verwendet habe, mit dem er die Website besucht hat. Ebenso sei unklar ob es eine dynamische oder statische IP-Adresse gewesen sei.

Doch selbst unter der Annahme, dass personenbezogene Daten vorliegen, sei bei der Beurteilung der Angemessenheit der Übermittlung in die USA ein risikobasierter Ansatz zu verfolgen. Dies sei aus den

„Schrems II“ FAQ des EDSA sowie aus der Entscheidung der Europäischen Kommission vom 4. Juni 2021 zu den neuen Standardvertragsklauseln abzuleiten. Im vorliegenden Fall sei zu berücksichtigen, dass die Übermittlung der verfahrensgegenständlichen Daten – wenn überhaupt – nur ein geringes Basisrisiko mit sich bringe. Es sei auch keine Offenlegung gemäß EO 12.333 gegeben, da die genannte Bestimmung die US-Regierung nicht autorisiere, Nutzerdaten von einem US-Anbieter zu erzwingen oder auch nur anzufordern, sie erhalte keine an Dienstanbieter außerhalb der USA gerichteten Vorgaben. Auch FISA § 702 sei angesichts der Verschlüsselung und der Anonymisierung von IP-Adressen irrelevant. Der Zweitbeschwerdegegner habe mit dem Erstbeschwerdegegner Standardvertragsklauseln abgeschlossen. Darüber hinaus habe er ergänzende Maßnahmen implementiert, um die Standardvertragsklauseln zu ergänzen.

Schließlich sei festzuhalten, dass eine Verletzung der Art. 44 ff DSGVO nicht im Rahmen einer Datenschutzbeschwerde geltend gemacht werden könne. Die Datenschutzbehörde habe auch keine Kompetenz, Rechtsverletzungen in der Vergangenheit festzustellen. Zudem seien die Art. 44 ff DSGVO nur für Datenexporteure anwendbar.

A.9. Mit Stellungnahme vom 3. Dezember 2021 brachte der Beschwerdeführer zusammengefasst Folgendes vor:

Es sei eine Verarbeitung von personenbezogenen Daten gegeben, dies sei u.a. durch die vorgelegten Beilagen belegt. Zur Kontokonfiguration im Google Konto habe man bereits im Parallelverfahren zur GZ: DSB-D155.027 eine Stellungnahme abgegeben.

Die gegenständliche IP-Anonymisierung erfolge erst nach der Übermittlung in die Sphäre von Google LLC. Dass diese zudem innerhalb des EWR erfolge, sei eine bloße Behauptung, die der Erstbeschwerdegegner als rechenschaftspflichtiger Verantwortlicher nachweisen müsse. Zudem sei für eine Zugriffsmöglichkeit durch US-Behörden nicht entscheidend, dass personenbezogene Daten tatsächlich geografisch den EWR verlassen. 50 U.S. Code § 1881a („FISA 702“) sei nicht auf in den geografisch in den USA verarbeitete Daten beschränkt, sondern beanspruche globale Geltung.

Darüber hinaus sei festzuhalten, dass speziell die Kombination von Cookie-Daten und IP-Adressen ein Tracking und die Auswertung geografischer Lokalisation, Internet-Anschluss und Kontext des Besuchers mit den bereits beschriebenen Cookie-Daten verknüpft werden könnten. Die DSGVO kenne in Kapitel V auch keinen „risikobasierten Ansatz“. Dieser finde sich nur in bestimmten Artikeln der DSGVO, wie etwa in Art. 32 leg.cit.

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-Nachrichtendienstes 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-Nachrichtendienste 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.10. Mit Stellungnahme vom 21. Dezember 2021 brachte die Erstbeschwerdegegnerin zusammengefasst Folgendes vor:

Wie bereits ausgeführt, habe sie Google Signals nicht eingesetzt. Als technisch eingesetzte Dienstleisterin habe der Zweitbeschwerdegegner in seiner Stellungnahme vom 2. November 2021 ausdrücklich festgehalten, dass eine IP-Anonymisierung grundsätzlich nur innerhalb des EWR stattfinde. Nur in Ausnahmefällen würden Webserver außerhalb des EWR genutzt. Im vorliegenden Fall wären normale Betriebsbedingungen vorgelegen.

A.11. Mit Stellungnahme vom 9. Februar 2022 wiederholte der Zweitbeschwerdegegner im Wesentlichen das bisherige Vorbringen.

Zudem wurde vorgebracht, dass die seitens des Beschwerdeführers vertretene Position besonders schwerwiegende und weitreichende praktische Folgen habe. Diese Position würde österreichischen Unternehmen, die am Weltmarkt tätig seien, als auch der gesamteuropäischen Wirtschaft einen schwerwiegenden Schaden zufügen. Die verfahrensgegenständlichen Webbrowser-bezogenen Daten seien nicht hinreichend spezifisch, um einen Browser „auszusondern“. US-Nachrichtendienste hätten hinsichtlich der verfahrensgegenständlichen Art von Google Analytics-Daten noch niemals eine Anordnung nach FISA 702 erlassen.

Es sei unzulässig, die Anwendung einer Beweislastumkehr auf die Frage des Personenbezugs der Daten anzunehmen. Die DSGVO kenne keine solche Beweislastumkehr. Darüber hinaus sei dies mit den Grundsätzen des österreichischen Verfahrensrechts und der Unschuldsvermutung unvereinbar.

Darüber hinaus existiere in Österreich keine Verbandsklagebefugnis nach Art. 80 Abs. 2 DSGVO und könne dies nicht dadurch umgangen werden, indem sich NOYB von einem ihrer Mitarbeiter zum Zweck der Führung eines „Musterverfahrens“ mandatieren lasse.

Der Stellungnahme waren zwei Dokumente als Beilage beigefügt.

A.9. Mit letzter Stellungnahme vom 1. März 2022 hat der Beschwerdeführer das bisherige Vorbringen im Wesentlichen wiederholt.



## **B. Beschwerdegegenstand**

B.1. Ausgehend vom Vorbringen des Beschwerdeführers ist erkennbar, dass Beschwerdegegenstand die Frage ist, ob die Erstbeschwerdegegnerin für die Übermittlung der personenbezogenen Daten des Beschwerdeführers an den Zweitbeschwerdegegner, die aufgrund der Implementierung des Tools Google Analytics auf ihrer Website [REDACTED] ausgelöst wurde, ein angemessenes Schutzniveau gemäß Art. 44 DSGVO gewährleistet hat.

So hat der Beschwerdeführer u.a. mit Stellungnahmen vom 11. Februar 2021 und vom 8. Juni 2021 gemäß § 24 Abs. 2 Z 5 DSG ausdrücklich die Feststellung beantragt, dass die gegenständlichen Datenübermittlungen nach Art. 44 DSGVO unzulässig waren.

B.2. 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.

B.3. Über den Antrag, gegen die Erstbeschwerdegegnerin (als Verantwortliche) nunmehr ein unverzügliches Verbot der Datenübermittlungen an den Zweitbeschwerdegegner zu verhängen, ist nicht abzusprechen, da diese das Tool Google Analytics zwischenzeitig von ihrer Website entfernt hat.

B.4. 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 im August 2020 Betreiberin der Dienstleistung [REDACTED]. Bei [REDACTED] handelt es sich um ein Online-Vergleichsportal, bei dem Produkte miteinander verglichen werden können. Auf diese Weise können Verbraucher für ein spezifisches Produkt den jeweils günstigsten Anbieter finden, der seitens der Erstbeschwerdegegnerin gelistet wird.

Die Erstbeschwerdegegnerin betreibt für den österreichischen Markt die Website [REDACTED]. Darüber hinaus betreibt die Erstbeschwerdegegnerin [REDACTED] auch für den deutschen Markt ([REDACTED]), den englischsprachigen Markt ([REDACTED]), den polnischen Markt ([REDACTED]) und den Markt im Vereinigten Königreich ([REDACTED]). Die Erstbeschwerdegegnerin ist nur in Österreich ansässig und besitzt keine weiteren Niederlassungen in anderen Mitgliedstaaten der Union.

*Beweiswürdigung zu C.1.: Die getroffenen Feststellungen beruhen auf der Stellungnahme der Erstbeschwerdegegnerin vom 22. Dezember 2020 (Frage 2) und wurden insofern nicht seitens des Beschwerdeführers bestritten. Darüber hinaus beruhen die getroffenen Feststellungen auf einer*

amtswegigen Recherche der Datenschutzbehörde unter [REDACTED] (abgefragt am 18. März 2022).

C.2. Der Zweitbeschwerdegegner hat das Tool Google Analytics entwickelt. Bei Google Analytics handelt es sich um einen Messdienst, der es Kunden des Zweitbeschwerdegegners u.a. 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.2.: Die getroffenen Feststellungen beruhen auf der Stellungnahme des Zweitbeschwerdegegners vom 9. April 2021 (S. 3 sowie Frage 1 und 2) und wurden seitens des Beschwerdeführers nicht bestritten. Die Stellungnahme des Zweitbeschwerdegegners vom 9. April 2021 wurde ursprünglich in einem Parallelverfahren zur GZ: [REDACTED] eingeholt und den Parteien des gegenständlichen Verfahrens zur Kenntnis gebracht, da es sich bei der Stellungnahme um allgemeine Ausführungen zur Funktionsweise von Google Analytics handelt.*

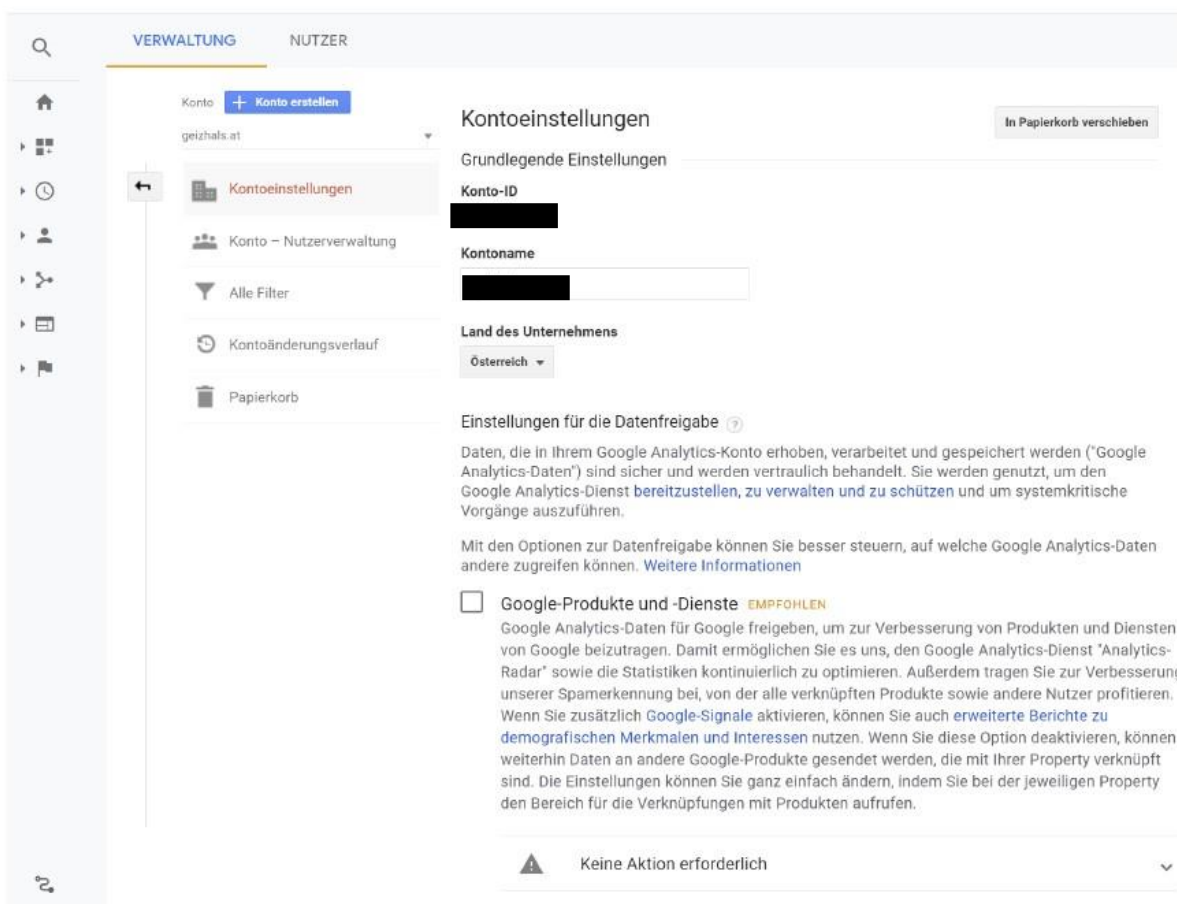
C.3. Die Erstbeschwerdegegnerin – als Website-Betreiberin – hat jedenfalls zum Stichtag 11. August 2020 die Entscheidung getroffen, die kostenlose Version des Tools Google Analytics für ihre „[REDACTED]“ Websites einzusetzen. Hierzu hat sie einen JavaScript Code („tag“), der seitens des Zweitbeschwerdegegners 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.

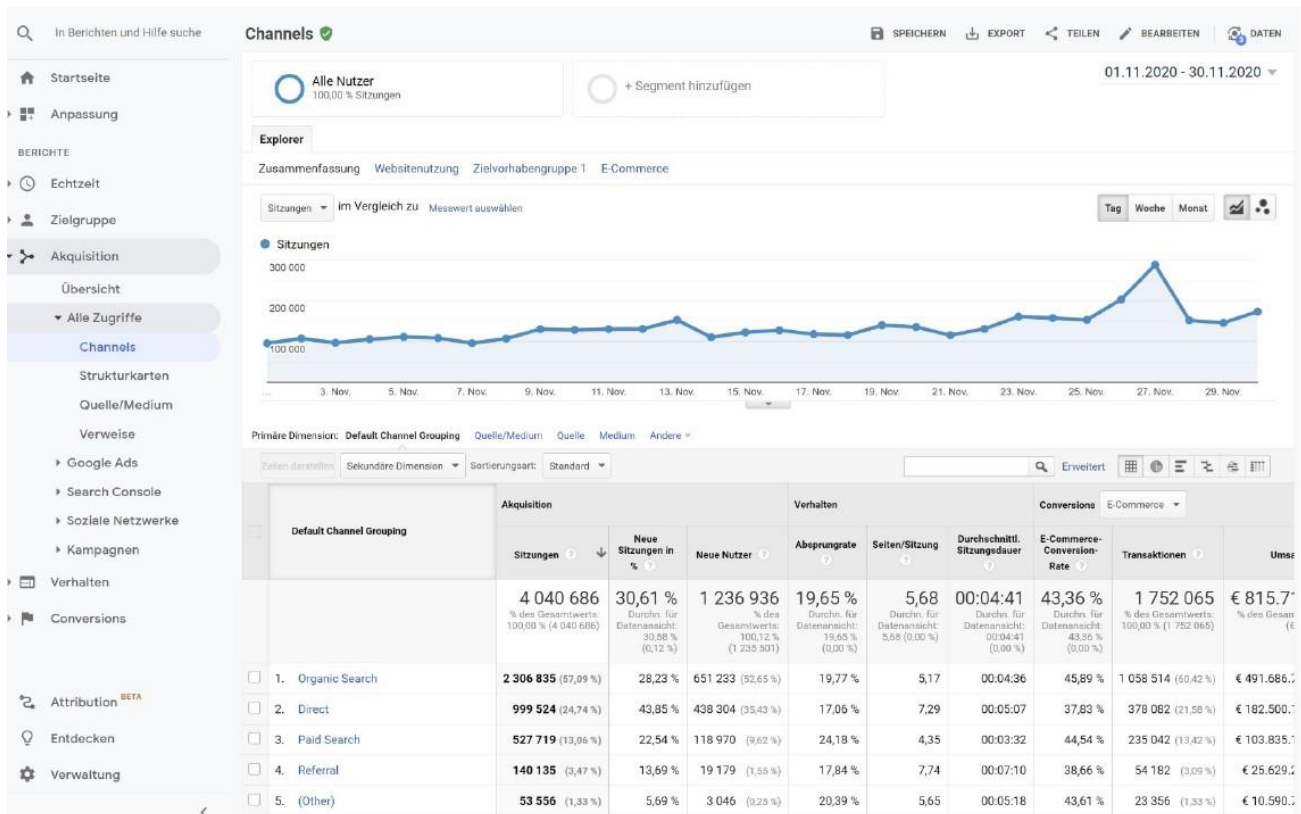
Diese Auswertungen werden seitens der Erstbeschwerdegegnerin jedenfalls dazu genutzt, um den Inhalt der Website [REDACTED] entsprechend dem allgemeinen Themeninteresse so darzustellen, dass die meistnachgefragten Channels in den Vordergrund gestellt und die Darstellung je nach Aktualität eines konkreten Themas angepasst werden kann.

Die Erstbeschwerdegegnerin hat hierzu ein Google Analytics Konto angelegt. Die Google Analytics Konto-ID mit dem Kontonamen „[REDACTED]“ lautet [REDACTED]. Die oben angeführten Auswertungen kann

die Erstbeschwerdegegnerin vornehmen, indem sie sich in das „[REDACTED]“ Google Analytics Konto einloggt und im Dashboard Berichte zum Traffic von [REDACTED] 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):





Beweiswürdigung zu C.3.: Die getroffenen Feststellungen beruhen auf der Eingabe der Erstbeschwerdegegnerin vom 22. Dezember 2020 und wurden seitens des Beschwerdeführers nicht bestritten. Die angeführten Screenshots wurden aus der vorgelegten Beilage ./B und ./D aufgenommen.

C.4. Das Tool Google Analytics hat folgende Funktionsweise: Wenn Besucher die Website [REDACTED] 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 DOMSchnittstelle 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 GIFAnfrageparameter 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 18. März 2022):

### 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_&lt;property-id&gt;</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_&lt;property-id&gt;</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. <a href="#">Learn more</a> .

**Beweiswürdigung zu C.4.: Die getroffenen Feststellungen beruhen auf der Stellungnahme des Zweitbeschwerdegegners vom 9. April 2021 (Frage 2) im Parallelverfahren zur GZ: [REDACTED] sowie einer amtswegigen Recherche der Datenschutzbehörde unter <https://developers.google.com/analytics/devguides/collection/gajs/cookie-usage> und auch**

<https://developers.google.com/analytics/devguides/collection/gtagjs/cookies-user-id> (beide abgefragt am 18. März 2022).

C.5. Die Beschwerdegegner haben einen Vertrag mit dem Titel „Auftragsverarbeiterbedingungen für Google Werbeprodukte“ abgeschlossen. Dieser Vertrag hatte in der Version vom 1. Jänner 2020 zumindest am 11. 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 1. Jänner 2020 (Stellungnahme der Beschwerdegegnerin vom 22. Dezember 2020, Beilage ./G) wird den Sachverhaltsfeststellungen zugrunde gelegt. Der genannte Vertrag wurde in Folge am 12. August 2020 sowie am 16. August 2020 aktualisiert.

Darüber hinaus haben Erst- und Zweitbeschwerdegegner 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 dieser Vertrag (Stellungnahme der Beschwerdegegnerin vom 22. Dezember 2020, Beilage ./K) wird den Sachverhaltsfeststellungen zugrunde gelegt.

Im ersten Vertrag wird hinsichtlich der von den „Auftragsverarbeiterbedingungen für Google Werbeprodukte“ erfassten Datenkategorien 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 18. März 2022):

## 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.5.:*** Die getroffenen Feststellungen beruhen auf der Stellungnahme des Erstbeschwerdegegners vom 22. Dezember 2020, Frage 15. Die angeführten Beilagen sind im Akt enthalten und sind allen Parteien bekannt. Darüber hinaus beruhen die getroffenen Feststellungen auf einer amtswegigen Recherche der Datenschutzbehörde unter <https://privacy.google.com/businesses/adsservices/> (abgefragt am 18. März 2022). Die getroffenen Feststellungen im Hinblick auf die „zusätzlich implementierten Maßnahmen“ ergeben sich aus der Stellungnahme des Zweitbeschwerdegegners vom 9. April 2021 (Frage 28) sowie aus der Stellungnahme der Erstbeschwerdegegnerin vom 22. Dezember 2020 (Frage 23). Die Stellungnahme des Zweitbeschwerdegegners vom 9. April 2021, die im Parallelverfahren zur GZ: ██████████ eingeholt wurde, ist im gegenständlichen 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-nationalsecurity?hl=en> (abgefragt am 18. März 2022).

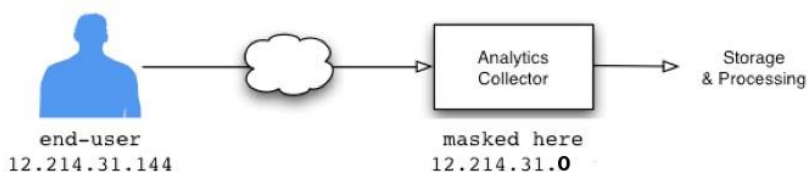
C.6. Im Zuge der Verwendung des Tools Google Analytics wird die Möglichkeit angeboten, eine „IPAnonymisierungsfunktion“ zu verwenden. Diese Funktion wurde seitens der Beschwerdegegnerin genutzt. Im Rahmen der Einbettung von Google Analytics auf der Website wurde die Funktion, „anonymizeIP“ auf „true“ gestellt. Beim Laden der relevanten Scripts von Google-Servern wird dennoch zunächst die vollständige IP-Adresse eines Website-Besuchers an den Zweitbeschwerdegegner übertragen. Die IP-Adresse wird erst in einem zweiten Schritt maskiert, nachdem sie im AnalyticsDatenerfassungsnetzwerk eingegangen ist.

Hierzu hat der Zweitbeschwerdegegner auf seiner Website unter <https://support.google.com/analytics/answer/2763052?hl=de> folgende Informationen zur Verfügung gestellt (Auszug, Formatierung nicht 1:1 wiedergegeben):

#### Detaillierte Informationen

In Analytics ist die Funktion `anonymize_ip` verfügbar (in der Bibliothek „gtag.js“ ist das `gtag('config', '<GA_MEASUREMENT_ID>', { 'anonymize_ip': true })`). Damit können Websiteinhaber anfordern, dass alle IP-Adressen ihrer Nutzer innerhalb des Produkts anonymisiert werden. So lassen sich eigene Datenschutzerklärungen oder die Empfehlungen der lokalen Datenschutzaufsichtsbehörden in einigen Ländern umsetzen, die unter Umständen das Speichern vollständiger IP-Adressen untersagen. Die IPs werden anonymisiert oder maskiert, sobald die Daten bei Google Analytics eingehen und noch bevor sie gespeichert oder verarbeitet werden.

Die IP-Anonymisierung in Analytics findet in zwei Schritten innerhalb des Datenerfassungssystems statt: über das JavaScript-Tag und im Datenerfassungsnetzwerk. Diese Schritte werden nachfolgend erläutert.



**Beweiswürdigung zu C.6.:** Die getroffenen Feststellungen beruhen auf der Stellungnahme der Erstbeschwerdegegnerin vom 22. Dezember 2020 (Frage 2) und der darin vorgelegten Beilage ./C. Aus Beilage ./C ist ersichtlich, dass der Zweitbeschwerdegegner selbst angibt, dass die Anonymisierung der IP-Adresse erst im zweiten Schritt nach der Datenerfassung erfolgt. Die Feststellung in Bezug auf den Zeitpunkt der Anonymisierung der IP-Adresse beruht darüber hinaus auf der Stellungnahme des Beschwerdeführers vom 11. Februar 2021 (S. 2 f). Schließlich beruhen die getroffenen Feststellungen auf einer amtswegigen Recherche der Website unter <https://support.google.com/analytics/answer/2763052?hl=de> (abgefragt am 18. März 2022). Wie aus der rechtlichen Beurteilung ersichtlich, kann es im Rahmen der Sachverhaltsfeststellung dahingestellt bleiben, ob die IP-Adresse des Endgeräts des Beschwerdeführers im gegenständlichen Fall innerhalb oder außerhalb des EWR-Raums maskiert wurde. Diesbezügliche Feststellungen konnten daher unterbleiben.



C.7. Der Beschwerdeführer besuchte zumindest am 11. August 2020 die Website [REDACTED]. Während des Besuchs war er in seinem Google-Konto eingeloggt. 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.7.: Die getroffenen Feststellungen beruhen auf der Eingabe des Beschwerdeführers vom 18. August 2020 (S. 2 f) 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 18. März 2022).*

C.8. In der beschwerdegegenständlichen Transaktion zwischen dem Browser des Beschwerdeführers und [REDACTED] wurden am 11. August 2020, um 01:26:21.206 MEZ einzigartige Nutzeridentifikations-Nummern zumindest in den Cookies „\_ga“ und „\_gid“ verarbeitet. In Folge wurden diese Kennnummern am 11. August 2020, um 01:26:23.795 MEZ an <https://www.googleanalytics.com/collect> 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 mit grün gekennzeichnet):

Domain	Name	Wert	Zweck
[REDACTED]	_ga	[REDACTED]	Google Analytics
[REDACTED]	_gid	[REDACTED]	Google Analytics

Diese Kennnummern enthalten jeweils am Ende den UNIX-Zeitstempel, aus dem sich ergibt, wann das jeweilige Cookie erstmalig gesetzt wurde. Die Kennnummer mit dem UNIX-Zeitstempel „1597101359“ wurde am Dienstag, 11. August 2020 um 01:15:59 MEZ gesetzt.

Dieselben Werte, wie in den Cookie-Dateien „\_ga“ und „\_gid“, waren im Anfrageinhalt („request payload“) zur Domain [www.google-analytics.com/collect](https://www.google-analytics.com/collect) enthalten (Hervorhebungen seitens der Datenschutzbehörde):

[REDACTED]

[REDACTED]

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 [REDACTED] 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 2020-0811T01:26:23.795+02:00):

#### General

[REDACTED]

#### Headers

[REDACTED]

- Host: [www.google-analytics.com](http://www.google-analytics.com)

[REDACTED]

[REDACTED]

[REDACTED]

- Headers 677 bytes
- Body 0 bytes
- Total 677 bytes

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 (IPV6-Adresse) [REDACTED], 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.8.: 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 13. August 2021 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 RemoteAdresse ergibt sich aus einer amtswegigen Who-Is-Abfrage der Datenschutzbehörde unter [REDACTED] (abgefragt am 18. März 2022).*

C.9. 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.9.: In seiner Stellungnahme vom 9. April 2021 im Parallelverfahren zur GZ: DSB-D155.027 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. Wie sich aus der rechtlichen Beurteilung gibt, ist eine solche Beweislastumkehr ausdrücklich in der DSGVO vorgesehen.

C.10. Die Erstbeschwerdegegnerin hat das Tool Google Analytics noch vor Abschluss des gegenständlichen Verfahrens von ihrer Website [REDACTED] entfernt.

Beweiswürdigung zu C.10.: Die getroffenen Feststellungen beruhen auf der Stellungnahme der Erstbeschwerdegegnerin vom 28. Mai 2021, die seitens des Beschwerdeführers insofern nicht bestritten wurde. Darüber hinaus beruht die Feststellung auf einer amtswegigen Recherche unter [REDACTED] (abgefragt am 18. März 2022).

## **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, ZI. 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.

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 entgegnen, 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**

Der Beschwerdeführer hat u.a. mit Stellungnahmen vom 11. Februar 2021 und vom 8. Juni 2021 gemäß § 24 Abs. 2 Z 5 DSG ausdrücklich die Feststellung beantragt, dass die gegenständlichen Datenübermittlungen nach Art. 44 DSGVO unzulässig waren.

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, Zl. 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) „schwerwiegende und weitreichende praktische Bedeutung“ des gegenständlichen Bescheids**

Der Zweitbeschwerdegegner hat in seiner letzten Stellungnahme vom 9. Februar 2022 zusammengefasst ausgeführt, dass ein der Beschwerde stattgebender Bescheid schwerwiegende Folgen für die Wirtschaft haben würde.

Diesbezüglich ist festzuhalten, dass der Datenschutzbehörde wirtschaftliche oder politische Überlegungen untersagt sind und diese nur punktuell im Rahmen der Auslegung der DSGVO – so etwa im Rahmen einer Interessenabwägung nach Art. 6 Abs. 1 lit. f leg. cit – zu berücksichtigen sind.

Die Datenschutzbehörde hat gemäß dem primärrechtlichen Art. 8 Abs. 3 EU-GRC und dem sekundärrechtlichen Art. 58 Abs. 1 lit. f DSGVO vielmehr die Verpflichtung, im Rahmen von datenschutzrechtlichen Beschwerden eine Entscheidung zu treffen, wobei dem Standpunkt des EuGH im Urteil vom 16. Juli 2020, Rs C.311/18, in Bezug auf die Rechtslage der USA Rechnung zu tragen war.

So hat der EuGH mit Urteil vom 16. Juli 2020 ausdrücklich festgehalten hat, dass die einschlägige Rechtslage in den USA – hierzu weiter unten – nicht mit dem Grundrecht auf Datenschutz gemäß Art. 8 EU-GRC vereinbar ist, weshalb auch der EU-USA Angemessenheitsbeschluss („Privacy Shield“) für ungültig erklärt wurde.

Eine wirtschaftliche oder politische Einigung für die Gewährleistung von Datenübermittlungen zwischen Europa und den USA haben andere Stellen – nicht jedoch Aufsichtsbehörden – zu erzielen. Das Vorbringen des Zweitbeschwerdegegners in Bezug auf die „schwerwiegende und weitreichende praktische Bedeutung“ des gegenständlichen Bescheids sowie die zitierten Wirtschaftsstudien müssen daher dahingestellt bleiben.

## **D.2. Spruchpunkt 1**

Die Datenschutzbehörde setzte das gegenständliche Verfahren mit Bescheid vom 2. Oktober 2020, Zl. D155.026, 2020-0.526.838, bis zur Feststellung, welche Behörde für die inhaltliche Verfahrensführung zuständig ist (federführende Aufsichtsbehörde) bzw. bis zur Entscheidung einer federführenden Aufsichtsbehörde oder des EDSA, aus.

Nach Auffassung der Datenschutzbehörde ist der Tatbestand des Art. 4 Z 23 lit. b DSGVO erfüllt, da die Erstbeschwerdegegnerin ihr Online-Vergleichsportal „[REDACTED]“ – wie festgestellt – auf den österreichischen ([REDACTED]), deutschen ([REDACTED]), polnischen ([REDACTED]) und englischsprachigen Markt ([REDACTED]) ausrichtet und unstrittig für alle Versionen von [REDACTED] die Website-Betreiberin ist. Somit war das Verfahren nach Art. 56 iVm Art. 60 ff DSGVO („One-Stop-Shop“) zu führen.

In Folge legte die Datenschutzbehörde – als federführende Aufsichtsbehörde – den betroffenen Aufsichtsbehörden einen Beschlussentwurf gemäß Art. 60 Abs. 3 DSGVO vor.



Da keine maßgeblichen und begründeten Einsprüche gegen den Beschlussentwurf vorgebracht wurden, war der Aussetzungsbescheid vom 2. Oktober 2020 zu beheben und den Parteien nach Art. 60 Abs. 7 und Abs. 8 DSGVO zu übermitteln.

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 auch 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.3. und C.8.), 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 [REDACTED] 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 ██████████ handelt. Mit anderen Worten: Erst der Einsatz solcher Kennnummern ermöglicht eine Unterscheidung von WebsiteBesuchern, 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 18. März 2022), 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 [REDACTED] 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.

An dieser Stelle ist zu bemerken, dass auch der Europäische Datenschutzbeauftragte (EDSB) die Auffassung vertritt, dass bei einem „Aussondern“ durch Markieren eines Endgeräts von personenbezogenen Daten auszugehen ist. So hat der EDSB in seiner Entscheidung vom 5. Jänner 2022, GZ: 2020-1013 gegen das Europäische Parlament u.a. Folgendes ausgeführt:

“[...] Tracking cookies, such as the Stripe and the Google analytics cookies, are considered personal data, even if the traditional identity parameters of the tracked users are unknown or have been deleted by the tracker after collection. All records containing identifiers that can be used to single out users, are considered as personal data under the Regulation and must be treated and protected as such.” (S. 13, Original in englischer Sprache und mit weiteren Nachweisen).

„[...] Tracking-Cookies wie die Stripe- und Google-Analytics-Cookies gelten als personenbezogene Daten, auch wenn die traditionellen Identitätsparameter der verfolgten Nutzer unbekannt sind oder vom Tracker nach der Erfassung gelöscht wurden. Alle Datensätze, die Identifizierungsmerkmale enthalten, mit denen Nutzer ausgesondert werden können, gelten nach der Verordnung als personenbezogene Daten und müssen als solche behandelt und geschützt werden“ (Übersetzung seitens der Datenschutzbehörde).

Zwar hat der EDSB die Verordnung (EU) 2018/1725 anzuwenden, die bei der Datenverarbeitung durch die Organe, Einrichtungen und sonstigen Stellen der Union gilt. Da Art. 3 Z 1 der Verordnung (EU) 2018/1725 der Definition von Art. 4 Z 1 DSGVO entspricht, können diese Überlegungen aber ohne weiteres auf den gegenständlichen Fall übertragen werden.

Als Zwischenergebnis ist daher festzuhalten, dass die hier gegenständlichen Google Analytics Kennnummern schon grundsätzlich als personenbezogene Daten (in Form einer Online-Kennung) gemäß Art. 4 Z 1 DSGVO zu qualifizieren sind.

### **c) Kombination mit weiteren Elementen**

Noch deutlicher erkennbar wird die Erfüllung des Tatbestands von Art. 4 Z 1 DSGVO, wenn man berücksichtigt, dass derartige 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 vollständige IP-Adresse jedenfalls für einen gewissen – wenn auch sehr kurzen – Zeitraum am Server von Google LLC verarbeitet wird. Dieser kurze Datenverarbeitungszeitraum ist ausreichend, damit der Tatbestand des Art. 4 Z 2 DSGVO erfüllt wird. Nach Judikatur des BVwG kann aus Art. 4 Z 2 iVm Art. 6 DSGVO nämlich nicht abgeleitet werden, dass von einer gewissen zeitlichen „Mindestverarbeitung“ auszugehen ist (vgl. das Erkenntnis des BVwG vom 3. September 2019, Zl. W214 2219944-1).

Wie noch an späterer Stelle ausgeführt wird, kann auf diese vollständige IP-Adresse – selbst wenn diese im konkreten Fall wie behauptet auf europäischen Servern des Zweitbeschwerdegegners verarbeitet wurde – seitens US-Nachrichtendienste zugegriffen werden.

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 aber 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.

#### **d) Rückführbarkeit auf den Beschwerdeführer**

Unabhängig von den obenstehenden Überlegungen ist aber ohnedies von einer Rückführbarkeit zum „Gesicht“ des Beschwerdeführers 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/Jotzo*, 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: die 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.

Insbesondere hat auch 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-D123.270/0009DSB/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.

#### **i) Dies ist zunächst der Zweitbeschwerdegegner:**

Wie sich aus den Sachverhaltsfeststellungen ergibt, war der Beschwerdeführer im Zeitpunkt des Besuchs der Website [REDACTED] mit seinem Google-Account 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 ein Benutzer, der im Google-Account des Beschwerdeführers eingeloggt war, die Website [REDACTED] besucht hat.

Selbst wenn man also die (nicht gebotene) Auffassung vertritt, dass die oben angeführten OnlineKennungen 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, zumal die Beschwerdegegner datenschutzrechtliche Verträge in Bezug auf Google Analytics abgeschlossen haben, die wiederum die Anwendbarkeit der DSGVO voraussetzen. Entsprechende Nachweise wurden – trotz mehrfach eingeräumter Möglichkeiten – jedoch nicht erbracht.

Anders als Kapitel V – hierzu weiter unten – stellen die Art. 5 Abs. 2 iVm Art. 24 Abs. 1 DSGVO nun tatsächlich auf einen risikobasierten Ansatz ab. Je höher nämlich das mit der Datenverarbeitung verbundene Risiko ist, desto höher ist der Maßstab an die vorzulegenden Beweise, um die Einhaltung der DSGVO nachzuweisen.

Im gegenständlichen Fall ist von einem hohen Risiko und daher von einem hohen Maßstab an die Beweispflicht auszugehen:

Der Zweitbeschwerdegegner hat das Produkt Google Analytics jedenfalls auch deshalb entwickelt, um möglichst viele Informationen von Websitebesuchern zu sammeln. So führt dieser selbst aus, dass aufgrund des Umstands, dass Google Analytics auf einer Website eingebettet ist, diese die Information erhalten kann, dass ein gewisser Google-Kontoinhaber eine solche Website besucht hat. Mit anderen Worten: Im Gegenzug dafür, dass Betreiber einer Website die kostenlose Version von Google Analytics verwenden können, erhält der Zweitbeschwerdegegner technische Möglichkeiten zur Datensammlung und zur weiteren Anreicherung der Profile von Google Kontoinhabern. Es ist daher nicht davon

auszugehen, dass es sich bei Google Analytics um einen bloßen Webanalysedienst für WebsiteBetreiber handelt.

Ausgehend von diesem hohen Maßstab an die Beweispflicht ist es nun nicht ausreichend, wenn bloß behauptet wird, dass der Zweitbeschwerdegegner die beschwerdegegenständlichen Informationen nur dann erhält, wenn im Google Konto gewisse Einstellungen ausgewählt werden. Weitere Beweise (etwa Screenshots, nähere technische Beschreibungen, u.ä.) wurden – trotz eines umfangreichen Ermittlungsverfahrens – nicht vorgelegt.

Nicht übersehen wird, dass die Rechenschaftspflicht gemäß Art. 5 Abs. 2 iVm Art. 24 Abs. 1 DSGVO ausdrücklich die Erstbeschwerdegegnerin als Verantwortliche trifft. Der stattgebende Teil des gegenständlichen Bescheids richtet sich aber gerade (nur) gegen die Erstbeschwerdegegnerin, welche das Produkt Google Analytics auf ihrer Website eingebettet hat.

Soweit der Zweitbeschwerdegegner in diesem Zusammenhang auf die Unschuldsvermutung gemäß Art. 48 Abs. 1 EU-GRC abstellt, ist dem entgegenzuhalten, dass es sich im gegenständlichen Fall ausschließlich um ein Beschwerdeverfahren nach Art. 77 Abs. 1 DSGVO und nicht um ein Verwaltungsstrafverfahren gehandelt hat. Davon abgesehen wurde die Beschwerde gegen den Zweitbeschwerdegegner ohnedies abgewiesen.

Wenn der Zweitbeschwerdegegner schließlich ausführt, dass eine solche „Beweislastverteilung“ mit dem österreichischen Verfahrensrecht nicht kompatibel sei, ist ihm entgegenzuhalten, dass es sich um eine ausdrückliche Regelung in der DSGVO handelt (Rechenschaftspflicht). Abgesehen davon ist eine solche „Beweislastverteilung“ in der Rechtsordnung – insbesondere im Verbraucherschutzrecht – durchaus üblich (vgl. etwa § 924 ABGB bzw. § 11 Abs. 1 VGG, BGBl. I Nr. 175/2021; zum engen Verhältnis zwischen dem Verbraucherschutzrecht und dem Grundrecht auf Datenschutz siehe auch ErwGr 42 DSGVO).

### **ii) 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 auch am – in den Sachverhaltsfeststellungen angeführten – Transparenzbericht des Zweitbeschwerdegegners, der belegt, dass es zu Datenanfragen von US-Behörden an den Zweitbeschwerdegegner kommt. Dabei können beispielsweise 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 Websitebetreiberin, die – trotz Veröffentlichung des genannten Urteils des EuGH vom 16. Juli 2020 – das Tool Google Analytics weiterhin eingesetzt hat.

Konkret wurde also die Informationen übermittelt, dass der Beschwerdeführer mit einem Endgerät, welches mit einer einzigartigen Google Analytics Kennnummer markiert wurde, zu einem bestimmten Zeitpunkt mit bestimmten Browsereinstellungen sowie einer bestimmten IP-Adresse eine bestimmte Website (hier: ein Vergleichsportal in Form von „“) besucht hat.

Zwar ist grundsätzlich richtig, dass es sich hierbei (zunächst) nur um Informationen über ein bestimmtes Endgerät handelt. Genauso wie jedoch mithilfe eines GPS-Tracker gewonnene Standortdaten eines Fahrzeugs zeitgleich auch personenbezogene Daten über den Aufenthalt des Fahrzeugfahrers darstellen können, stellen die hier relevanten Informationen personenbezogene Daten jener Person dar, die das Endgerät am wahrscheinlichsten verwendet hat.

Dies ist im gegenständlichen Fall der Beschwerdeführer, zumal er im Zeitpunkt des Aufrufs der Website (unstrittig) im Browser mit dem persönlichen Google Konto angemeldet war. Anhaltspunkte dafür, dass der Beschwerdeführer seine Zugangsdaten an Dritte übergeben hat, sind nicht vorhanden und wurde dies – soweit ersichtlich – auch von keiner Partei behauptet.

Ein Maßstab dahingehend, dass mit „Sicherheit“ feststehen muss, welche natürliche Person das Endgerät verwendet hat, kann nicht aus Art. 4 Z 1 DSGVO abgeleitet werden und ist auch nicht geboten:

Bei dieser Betrachtung wären nämlich zu einem Endgerät bzw. einem Account gehörende Informationen immer nicht-personenbezogene Daten, da grundsätzlich nie ausgeschlossen werden kann, dass das Endgerät bzw. Zugangsdaten an Dritte (etwa Freunde oder Familienangehörige) weitergegeben wurden. Eine derartige Ansicht würde zu einem zu eng gefassten Anwendungsbereich von Art. 4 Z 1 DSGVO führen, was wiederum im Widerspruch zur Judikatur des EuGH steht, der von einem sehr weiten Anwendungsbereich ausgeht.



Als weiteres Zwischenergebnis ist daher festzuhalten, dass es sich bei den in den Sachverhaltsfeststellungen unter C.8. 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 [REDACTED] 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. die Stellungnahme vom 22. 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.8. angeführten Informationen (durch Google Ireland Limited oder dem Zweitbeschwerdegegner) ist nicht Beschwerdegegenstand und wurde somit auch nicht näher in diese Richtung ermittelt.

Die datenschutzrechtliche Rolle des Zweitbeschwerdegegners ist für das gegenständliche Verfahren daher nicht weiter von Relevanz, zumal die Pflicht zur Einhaltung von Art. 44 DSGVO Verantwortliche und Auftragsverarbeiter gleichermaßen trifft.

### **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 („Datenimporteuer“);
- der Datenimporteuer befindet sich in einem Drittland oder ist eine internationale Organisation, unabhängig davon, ob dieser Datenimporteuer in Bezug auf die betreffende Verarbeitung gemäß Art. 3 der DSGVO unterliegt oder nicht.

Die Erstbeschwerdegegnerin hat ihren Sitz in Österreich und ist für den Betrieb der Website [REDACTED] 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 [REDACTED] implementiert hat und als direkte Folge dieser Implementierung u.a. eine Datenübermittlung an den Zweitbeschwerdegegner (in die USA) stattfand. Schließlich hat der Zweitbeschwerdegegner seinen Sitz in den USA.

Somit sind die (in der aktuellen Fassung der Leitlinien des EDSA durchaus eng definierten) Voraussetzungen erfüllt und unterliegt die Erstbeschwerdegegnerin als Datenexporteurin jedenfalls 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 Sachverhaltsfeststellung C.5. ergibt, haben die Beschwerdegegner 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 [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).

Für die Datenschutzbehörde bestehen keine Zweifel, 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 (vgl. auch das seitens der DSK in Auftrag gegebene Rechtsgutachten vom 15. November 2021 zum aktuellen Stand des USÜberwachungsrechts und der Überwachungsbefugnisse von *Vladeck*, Frage 5 f, wonach der Anwendungsbereich von FISA 702 sehr weit zu verstehen ist und sich die Befugnisse von US-Behörden aufgrund einer geringfügigen Tätigkeit im Anwendungsbereich von FISA 702 auf sämtliche Daten im Unternehmen erstrecken).

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 18. März 2022).

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 (vgl. 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 V. 2.0“ 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).

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 52):

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 99).

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 im EWR gewährleisteten Schutzniveau im Wesentlichen gleichwertig ist (ebd. Rz 128).

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 79).

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 75).

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 81).

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 „Anonymisierungsfunktion der IP-Adresse“ ist nicht effektiv, da die Daten – wie oben näher ausgeführt – zumindest einen gewissen Zeitraum seitens des Zweitbeschwerdegegners verarbeitet werden. Selbst unter der Annahme, dass die IP-Adresse innerhalb des Zeitraums nur in Servern im EWR verarbeitet wurde, ist darauf hinzuweisen, dass der Zweitbeschwerdegegner nach dem einschlägigen Recht der USA trotzdem von US-Nachrichtendiensten zur Herausgabe der IP-Adresse verpflichtet werden kann (vgl. hierzu ausführlich die EDPB-EDPS Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection [annex] vom 10. Juli 2019, S. 1 f; vgl. das bereits erwähnte Rechtsgutachten vom 15. November 2021 von *Vladeck*, Frage 8 ff, wonach auch FISA 702 extraterritorial angewendet werden kann).

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) Kapitel V DSGVO kennt keinen risikobasierten Ansatz**

Der Zweitbeschwerdegegner bringt in weiterer Folge – zusammengefasst – vor, dass das Risiko der Datenübermittlung in die USA zu berücksichtigen sei und die belangte Behörde einen zu strengen Maßstab verfolge. Diesen Ausführungen ist nicht zu folgen:

Aus dem Wortlaut von Art. 44 DSGVO kann ein solch „risikobasierter Ansatz“ nicht abgeleitet werden:

#### *Art. 44 DSGVO*

#### **Allgemeine Grundsätze der Datenübermittlung**

Jedwede Übermittlung personenbezogener Daten, die bereits verarbeitet werden oder nach ihrer Übermittlung an ein Drittland oder eine internationale Organisation verarbeitet werden sollen, ist 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.

Aus dem Wortlaut von Art. 44 DSGVO ist vielmehr abzuleiten, dass für jede Datenübermittlung an ein Drittland (oder an eine internationale Organisation) sichergestellt werden muss, dass das durch die DSGVO gewährleistete Schutzniveau nicht untergraben wird.

Der Beschwerdeerfolg einer Verletzung von Art. 44 DSGVO hängt daher nicht davon ab, ob ein gewisses „Mindestrisiko“ gegeben ist, oder ob US-Nachrichtendienste tatsächlich auf Daten zugegriffen haben. Eine Verletzung von Art. 44 DSGVO liegt nach dem Wortlaut dieser Bestimmung bereits dann vor, wenn personenbezogene Daten in ein Drittland ohne ein entsprechendes Schutzniveau übermittelt werden.



Im Zusammenhang mit jenen Vorgaben der DSGVO, wo tatsächlich ein risikobasierter Ansatz zu verfolgen ist („je höher das Verarbeitungsrisiko, desto mehr Maßnahmen sind zu implementieren“), hat der Verordnungsgeber dies auch ausdrücklich und ohne Zweifel normiert. So ist der risikobasierte Ansatz beispielhaft in Art. 24 Abs. 1 und Abs. 2, Art. 25 Abs. 1, Art. 30 Abs. 5, Art. 32 Abs. 1 und Abs. 2, Art. 34 Abs. 1, Art. 35 Abs. 1 und Abs. 3 oder Art. 37 Abs. 1 lit. b und lit. c DSGVO vorgesehen.

Da der Verordnungsgeber an zahlreichen Stellen der DSGVO einen risikobasierten Ansatz normiert hat, im Zusammenhang mit den Vorgaben von Art. 44 DSGVO jedoch nicht, kann nicht davon ausgegangen werden, dass der Verordnungsgeber dies bloß „übersehen“ hat; eine analoge Anwendung des risikobasierten Ansatzes auf Art. 44 DSGVO ist somit ausgeschlossen.

Auch der Verweis auf den „freien Datenverkehr“ vermag für den Standpunkt der Beschwerdeführerin nichts zu gewinnen:

Es ist unstrittig, dass die DSGVO (auch) den freien Datenverkehr gewährleisten soll. Der freie Datenverkehr steht aber eben unter der Prämisse, dass die Vorgaben der DSGVO – und hierzu zählt auch Kapitel V – vollständig eingehalten werden. Ein Aufweichen im Sinne einer „wirtschaftsfreundlichen Interpretation“ der Vorgaben von Kapitel V zugunsten des freien Datenverkehrs ist nicht vorgesehen. Wirtschaftliche Interessen spielten auch im bereits erwähnten Urteil des EuGH vom 16. Juli 2020 keine Rolle.

Die weitere Argumentation, dass der „risikobasierte Ansatz vom EuGH mit Urteil vom 16. Juli 2020 bestätigt wurde“, kann nicht nachvollzogen werden:

Der EuGH ist in seiner Analyse der Rechtslage der USA und zur Gültigkeit des EU-USA Angemessenheitsbeschlusses gerade nicht von einem risikobasierten Ansatz in Kapitel V DSGVO ausgegangen. Tatsächlich wird ein solch risikobasierter Ansatz im genannten Urteil nicht erwähnt.

Der Zweitbeschwerdegegner leitet offenbar aus der seitens des EuGH verwendeten Wortfolge „angemessenes Datenschutzniveau“ einen risikobasierten Ansatz ab. Dem ist nicht zu folgen, da der EuGH diese Wortfolge unter Bezug auf ErwGr 108 DSGVO verwendet hat. Aus ErwGr 108 der Verordnung ist ersichtlich, dass „angemessenes Datenschutzniveau“ bedeutet, dass die Rechte der betroffenen Personen auf eine angemessene Art und Weise zu beachten sind.

Der EuGH ist in Bezug auf die Rechtslage der USA nun gerade davon ausgegangen, dass aufgrund der unverhältnismäßigen Zugriffsmöglichkeiten von US-Behörden gerade von keinem „angemessenen Datenschutzniveau“ auszugehen ist, weshalb er schließlich auch den EU-USA Angemessenheitsbeschluss für ungültig erklärt hat.

Der EuGH hat ausdrücklich nicht darauf abgestellt, dass die Verpflichtungen, denen sich ein PrivacyShield zertifiziertes Unternehmen aus den USA unterwirft, im Einzelfall möglicherweise doch

angemessen sind (etwa, weil das zertifizierte Unternehmen bloß nicht-sensible oder nicht-strafrechtlich relevante personenbezogene Daten erhält).

Ebenso kann die Argumentation, dass die Europäische Kommission sich in ihrem Durchführungsbeschluss (EU) 2021/914, mit welchem neue Standardvertragsklauseln verabschiedet wurden, „ebenso klar für einen risikobasierten Ansatz ausgesprochen hat“, nicht nachvollzogen werden:

Festzuhalten ist, dass auch der Durchführungsbeschluss (EU) 2021/914 keinen risikobasierten Ansatz enthält. Der nunmehrige Durchführungsbeschluss, der in Folge des Urteils des EuGH vom 16. Juli 2020 erlassen wurde, setzt gemäß dessen Art. 14 – im Gegenteil – voraus, dass die Vertragsparteien von Standarddatenschutzklauseln nun vor der Datenübermittlung in ein Drittland die lokalen Rechtsvorschriften und Pflichten im Falle des Zugangs von Behörden zu den Daten zu überprüfen haben.

Soweit der Zweitbeschwerdegegner den vermeintlichen Standpunkt der Europäischen Kommission aus dem (nicht verbindlichen) ErwGr 20 des genannten Durchführungsbeschlusses ableitet, ist ihm entgegenzuhalten, dass auch in ErwGr 20 von keinem risikobasierten Ansatz ausgegangen wird:

ErwGr 20 des genannten Durchführungsbeschlusses stellt richtigerweise darauf ab, dass im Rahmen der Beurteilung des Datenschutzniveaus in einem Drittstaat insbesondere die Umstände der Übermittlung zu berücksichtigen sind.

Umgelegt auf das Beispiel der Rechtslage der USA ist etwa zu überprüfen, ob im Einzelfall Daten an einen Anbieter elektronischer Kommunikationsdienste im Sinne von 50 U.S. Code § 1881(b)(4) übermittelt werden, andernfalls die entsprechenden Zugriffsmöglichkeiten von nach FISA 702 keine Anwendung finden. Wäre Österreich ein Drittstaat, so müsste man vor Datenübermittlungen nach Österreich überprüfen, ob die konkret übermittelten Datenarten etwa dem Anwendungsbereich nach dem (nunmehrigen) Staatsschutz- und Nachrichtendienst-Gesetz, BGBl. I Nr. 5/2016 idGF., unterliegen und ob die Zugriffsmöglichkeiten der Direktion Staatsschutz- und Nachrichtendienst verhältnismäßig sind.

Dabei handelt es sich aber (nur) um eine Prüfung, ob die lokalen Rechtsvorschriften und Pflichten im Falle des Zugangs von Behörden zu den Daten den vertraglichen Pflichten der Standarddatenschutzklauseln entgegenstehen und nicht um einen risikobasierten Ansatz in dem Sinne, dass zu überprüfen ist, wie sensibel oder nicht-sensibel die übermittelten personenbezogenen Daten sind.

Im Übrigen ist festzuhalten, dass ein Durchführungsbeschluss der Europäischen Kommission den Vorgaben von Art. 44 DSGVO ohnedies keinen völlig neuen Inhalt unterstellen könnte (vgl. zum Vorrang des Verordnungstextes etwa das Urteil des EuGH vom 12. Mai 2005, C-444/03, Rn 25).

Schließlich vermag auch der Verweis auf die Empfehlungen 01/2020 des EDSA zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten nichts für den Standpunkt der Beschwerdeführerin zu gewinnen:

So besagt die seitens des Zweitbeschwerdegegners zitierte Stelle der Empfehlungen – wie bereits im Zusammenhang mit dem Durchführungsbeschluss (EU) 2021/914 ausgeführt – nur, dass bei jeder Datenübermittlung zu überprüfen ist, ob die problematischen Gesetze des Drittlandes zur Anwendung gelangen und gerade nicht, dass zu überprüfen wäre, wie sensibel oder nicht-sensibel die übermittelten personenbezogenen Daten sind.

Soweit der Zweitbeschwerdegegner schließlich vorbringt, dass US-Nachrichtendienste gar kein Interesse an den gegenständlich verarbeiteten Daten hätten – indem etwa ausgeführt wird, dass es sich bei der Information zur „Bildschirmauflösung um einen Industriestandard handelt“ – ist dem entgegenzuhalten, dass es nicht auf ein allfälliges Interesse von US-Nachrichtendienste ankommt, sondern auf deren Zugriffsmöglichkeiten.

Unabhängig davon ist aber festzuhalten, dass der Mehrwert der Informationen insbesondere darin liegt, dass diese kombiniert werden können (vgl. hierzu auch die Definition von „Fingerprinting“ gemäß RFC6973 des Internet Architecture Board, wonach „Fingerprinting“ der Vorgang ist, bei dem ein Beobachter ein Gerät oder eine Anwendungsinstanz mit ausreichender Wahrscheinlichkeit auf Grundlage mehrerer Informationselemente identifiziert). Ebenso kann beispielsweise allein anhand der verarbeiteten IP-Adresse – als Bestandteil des digitalen Fußabdrucks – herausgefunden werden, welcher Internet-Provider genutzt wird und in welcher Region sich der Benutzer des Endgeräts aufhält.

## **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 [REDACTED] 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.

Von den Abhilfebefugnissen war aber nicht Gebrauch zu machen, da das Tool vor Abschluss des gegenständlichen Beschwerdeverfahrens entfernt wurde.

### **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.

## RECHTSMITTELBELEHRUNG

Gegen diesen Bescheid kann innerhalb von **vier Wochen** nach Zustellung schriftlich eine Beschwerde an das Bundesverwaltungsgericht erhoben werden. Die Beschwerde **ist bei der Datenschutzbehörde einzubringen** und muss

- die Bezeichnung des angefochtenen Bescheides (GZ, Betreff)
- die Bezeichnung der belangten Behörde,
- die Gründe, auf die sich die Behauptung der Rechtswidrigkeit stützt,
- das Begehren sowie
- die Angaben, die erforderlich sind, um zu beurteilen, ob die Beschwerde rechtzeitig eingebracht ist, enthalten.

Die Datenschutzbehörde hat die Möglichkeit, innerhalb von zwei Monaten entweder durch **Beschwerdevorentscheidung** ihren Bescheid abzuändern oder die Beschwerde mit den Akten des Verfahrens **dem Bundesverwaltungsgericht vorzulegen**.

Die Beschwerde gegen diesen Bescheid ist **gebührenpflichtig**. Die feste Gebühr für eine entsprechende Eingabe samt Beilagen beträgt **30 Euro**. Die Gebühr ist unter Angabe des Verwendungszwecks auf das Konto des Finanzamtes Österreich zu entrichten.

Die Gebühr ist grundsätzlich elektronisch mit der Funktion „Finanzamtszahlung“ zu überweisen. Als Empfänger ist das Finanzamt Österreich - Dienststelle Sonderzuständigkeiten anzugeben oder auszuwählen (IBAN: AT83 0100 0000 0550 4109, BIC: BUNDATWW). Weiters sind die Steuernummer/Abgabenkontonummer 10 999/9102, die Abgabenart „EEE -Beschwerdegebühr“, das Datum des Bescheides als Zeitraum und der Betrag anzugeben.

Sofern das e-banking-System Ihres Kreditinstituts nicht über die Funktion „Finanzamtszahlung“ verfügt, kann das eps-Verfahren in FinanzOnline genutzt werden. Von einer elektronischen Überweisung kann nur dann abgesehen werden, wenn bisher kein e-banking-System genutzt wurde (selbst wenn der Steuerpflichtige über einen Internetanschluss verfügt). Dann muss die Zahlung mittels Zahlungsanweisung erfolgen, wobei auf die richtige Zuordnung zu achten ist. Weitere Informationen erhalten Sie beim Finanzamt und im Handbuch „*Elektronische Zahlung und Meldung zur Zahlung von Selbstbemessungsabgaben*“.

Die Entrichtung **der Gebühr** ist bei Einbringung der Beschwerde **gegenüber der Datenschutzbehörde** durch einen der Eingabe anzuschließenden Zahlungsbeleg oder einen Ausdruck über die erfolgte Erteilung einer Zahlungsanweisung **nachzuweisen**. Wird die Gebühr nicht oder nicht vollständig entrichtet, ergeht eine **Meldung an das zuständige Finanzamt**.

Eine rechtzeitig eingebrachte und zulässige Beschwerde an das Bundesverwaltungsgericht hat **aufschiebende Wirkung**. Die aufschiebende Wirkung kann im Spruch des Bescheids ausgeschlossen worden sein oder durch einen eigenen Bescheid ausgeschlossen werden.

22. April 2022

Für die Leiterin der Datenschutzbehörde:

■■■■■■■■■■