BVwG
Bundesverwaltungsgericht
Republik Österreich

Postadresse:
Erdbergstraße 192 – 196
1030 Wien
Tel: +43 1 601 49 – 0
Fax: + 43 1 711 23-889 15 41
E-Mail: einlaufstelle@bvwg.gv.at
www.bvwg.gv.at

Entscheidungsdatum
12.05.2023
Geschäftszahl

W245 2252208-1/36E
W245 2252221-1/30E

Schriftliche Ausfertigung des am 31.03.2023 mündlich verkündeten Erkenntnisses

I M N A M E N D E R R E P U B L I K !

Das Bundesverwaltungsgericht hat durch den Richter Mag. Bernhard SCHILDBERGER, LL.M. als Vorsitzenden sowie Mag.[a] Viktoria HAIDINGER als fachkundige Laienrichterin und Mag. Thomas GSCHAAR als fachkundigen Laienrichter über die Beschwerden von XXXX , vertreten durch XXXX und XXXX , vertreten durch Baker & McKenzie Rechtsanwälte LLP & Co KG, Schottenring 25, 1010 Wien gegen den Teilbescheid der Österreichischen Datenschutzbehörde vom 22.12.2021, GZ 2021-0.586.257 (DSB-D155.027), betreffend die Verletzung der allgemeinen Grundsätze der Datenübermittlung gemäß Art. 44 DSGVO, nach Durchführung einer mündlichen Verhandlung, zu Recht erkannt:

A)

I. Die Beschwerde von XXXX gegen Spruchpunkt 2. des bekämpften Teilbescheides wird zurückgewiesen.

II. Die Revision ist gemäß Art. 133 Abs. 4 B-VG zulässig.

B)

I. Die Beschwerde von XXXX gegen Spruchpunkt 3. des bekämpften Teilbescheides wird abgewiesen.

II. Die Revision ist gemäß Art. 133 Abs. 4 B-VG zulässig.

Entscheidungsgründe:

Verfahrensgegenstand:

Der Beschwerdeführer XXXX (in der Folge auch „BF1“) besuchte am 14.08.2020 eine Website XXXX der Mitbeteiligten XXXX (in der Folge auch „MB“). Auf der Website des MB war der Webanalysedienst XXXX Analytics der Beschwerdeführerin XXXX (in der Folge auch „BF2“) eingebettet. Mit dem eingebetteten Webanalysedienst wurden personenbezogene Daten des BF1 in ein Drittland transferiert. Die gegenständliche Entscheidung behandelt die Frage, ob es mit der verfahrensgegenständlichen Verarbeitung zu einer Verletzung der allgemeinen Grundsätze der Datenübermittlung gemäß Art. 44 DSGVO gekommen ist.

= Google Analytics

= Google

Websiten-besucher =

I. Verfahrensgang:

I.1. Mit Eingabe vom 18.08.2020 brachte der BF1 eine Beschwerde gegen die BF2 und die MB ein (VWA ./01, siehe Punkt II.2).

Begründend führte der BF1 aus, dass er am 14.08.2020, um 10:45 Uhr die Website der MB XXXX besucht habe. Während des Besuchs der Website der MB sei der BF1 auf einem XXXX -Konto eingeloggt gewesen. Dieses Konto sei mit der E-Mail-Adresse des BF1 (XXXX verknüpft gewesen. Die MB habe auf ihrer Website den HTML-Code für XXXX -Dienste (einschließlich XXXX -Analytics) eingebettet gehabt.

Im Verlauf des Besuchs auf der Website der MB habe der BF1 personenbezogene Daten des BF1 (zumindest die IP-Adresse des BF1 und Cookie Daten) verarbeitet. Offenbar seien diese an die BF2 übermittelt worden (VWA ./04).

Gemäß Punkt 10 der Auftragsdatenverarbeitungsbedingungen habe die MB zugestimmt, dass die BF2 personenbezogene Daten des BF1 in den Vereinigten Staaten von Amerika oder in einem anderen Land, in dem XXXX oder XXXX Unterauftragsverarbeiter Einrichtungen unterhalte, speichern und verarbeiten könne. Eine solche Übertragung der personenbezogenen Daten des BF1 von der MB an die BF2 erfordere eine Rechtsgrundlage gemäß Art. 44 ff DSGVO.

Nachdem der Europäische Gerichtshof das „EU-US Privacy Shield“ mit der Entscheidung vom 16.07.2020, C-311/18 (*Schrems II*) für ungültig erklärt habe, könne die MB die Datenübermittlung an die BF2 in die Vereinigten Staaten nicht mehr auf eine Angemessenheitsentscheidung nach Art. 45 DSGVO stützen. Dennoch hätten sich die MB und

die BF2 nach dem Urteil noch fast vier Wochen auf das für ungültig erklärte „EU-US Privacy Shield“ berufen. Dies könne man aus Punkt 10.2 der Auftragsdatenverarbeitungsbedingungen für XXXX Werbeprodukte, Version 01.01.2020 entnehmen (VWA ./03).

Außerdem könne die MB die Datenübermittlung auch nicht auf Standarddatenschutzklauseln gemäß Art. 46 Abs. 2 lit. c und d DSGVO stützen, wenn das Bestimmungsdrittland nach Maßgabe des Unionsrechts keinen angemessenen Schutz der auf der Grundlage von Standarddatenschutzklauseln übermittelten personenbezogenen Daten gewährleiste (EuGH 16.07.2020, C-311/18 (Schrems II), Rn 134 f). Der EuGH habe ausdrücklich festgehalten, dass weitere Übermittlungen an Unternehmen, welche unter 50 U.S. Code § 1881a fallen, nicht nur gegen die einschlägigen Artikeln in Kapitel V DSGVO, sondern auch gegen Art. 7 und 8 GRC verstoßen sowie den Wesensgehalt von Art. 47 GRC verletzen würden (EuGH 06.10.2015, C-362/14 (*Schrems*), Rn 95). Jede weitere Übermittlung verstoße daher gegen das Grundrecht auf Privatsphäre und auf Datenschutz sowie das Recht auf einen wirksamen Rechtsbehelf und ein faires Verfahren.

Die BF2 sei als Anbieter elektronischer Kommunikationsdienste im Sinne von 50 U.S. Code § 1881a (b) (49) zu qualifizieren und unterliege als solcher der Überwachung durch US-Geheimdienste gemäß 50 U.S. Code § 1881a („FISA 702“): Wie aus den „ XXXX “ (VWA ./06) und aus dem Transparenzbericht der BF2 (siehe XXXX hervorgehe, stelle die BF2 der US-Regierung gemäß 50 U.S. Code § 1881a aktiv personenbezogene Daten zur Verfügung. Vor diesem Hintergrund sei die MB nicht in der Lage, einen angemessenen Schutz der personenbezogenen Daten des BF1, welche an die BF2 übermittelt werden, zu gewährleisten.

Ab 12.08.2020 haben sich die MB und die BF2 bei Datenübermittlungen in die Vereinigten Staaten auf Standdatenschutzklauseln berufen. Dies könne man Punkt 10.2 der Auftragsdatenverarbeitungsbedingungen für XXXX Werbeprodukte, Version 12.08.2020, entnehmen (VWA ./04). Diese Vorgangsweise ignoriere jedoch das Urteil des Europäischen Gerichtshofes (EuGH 16.07.2020, C-311/18 (*Schrems II*), Rn 134 f). Demnach sei die MB verpflichtet, die Übermittlung von personenbezogenen Daten an die BF2 in den Vereinigten Staaten zu unterlassen.

Schließlich akzeptiere die BF2 trotz des eindeutigen Urteils des Europäischen Gerichtshofes und unter Verletzung der Art. 44 bis 49 DSGVO weiterhin Datenübermittlungen aus der EU/EWR im Rahmen der Datenschutzklauseln. Darüber hinaus gebe die BF2 personenbezogene Daten aus der EU/EWR an die US-Regierung weiter und verstoße damit gegen Art. 48 DSGVO.

Der BF1 beantragte gemäß Art. 58 Abs. 1 DSGVO, dass festgestellt werde, welche personenbezogenen Daten von der MB an die BF2 in die Vereinigten Staaten oder an ein anders Drittland oder eine internationale Organisation übermittelt worden seien, auf welchen Übermittlungsmechanismus gemäß Art. 44 ff DSGVO die MB die Datenübermittlung gestützt habe und ob die Bestimmungen der anwendbaren Nutzungsbedingungen für XXXX -Analytics und der (neuen) Auftragsdatenverarbeitungsbedingungen für XXXX Werbeprodukte die Anforderungen von Art. 28 DSGVO in Bezug auf die Übermittlung personenbezogener Daten erfüllen oder nicht.

Ferner beantragte der BF1 das gemäß Art. 58 Abs. 2 lit. d, f und j DSGVO unverzüglich ein Verbot oder eine Aussetzung jeglicher Datenübermittlung von der MB an die BF2 in die Vereinigten Staaten verhängt sowie die Rückgabe dieser Daten an die EU/EWR oder ein anderes Land, das einen angemessenen Schutz gewährleiste, angeordnet werde.

Schließlich beantragte der BF1 die Verhängung einer wirksamen, verhältnismäßigen und abschreckenden Geldbuße gegen die MB und die BF2.

Seiner Beschwerde an die bB legte der BF1 Nutzungsbedingungen für XXXX -Analytics (VWA ./02, siehe Punkt II.2), die Auftragsdatenverarbeitungsbedingungen für XXXX Werbeprodukte, Version 01.01.2020 (VWA ./03, siehe Punkt II.2), die Auftragsdatenverarbeitungsbedingungen für XXXX Werbeprodukte, Version 12.08.2020 (VWA ./04, siehe Punkt II.2), die HAR-Daten des Website-Besuchs (VWA ./05, siehe Punkt II.2), die XXXX (VWA ./06, siehe Punkt II.2) sowie eine Vertretungsurkunde (VWA ./07, siehe Punkt II.2) bei.

I.2. In der Folge setzte die bB das Verfahren bis zur Feststellung der federführenden Aufsichtsbehörde und bis zur Entscheidung der federführenden Aufsichtsbehörde bzw. des Europäischen Datenschutzausschusses mit Bescheid vom 02.10.2020, Zl 2020-0.527.385 (DSB-D155.027) aus (VWA ./08 und ./09, siehe Punkt II.2). Ferner forderte die bB die MB zur Stellungnahme auf (VWA ./10, siehe Punkt II.2).

I.3. In der Stellungnahme vom 16.12.2020 führte die MB aus (VWA ./11, siehe Punkt II.2), dass sie sich selbst dafür entschieden habe, den Programmcode für XXXX -Analytics (in der Folge auch „Tool“ genannt) auf ihrer XXXX einzubetten. Das Tool werde dafür eingesetzt, um statistische Auswertungen über das Verhalten der Websitebesucher zu ermöglichen (siehe Punkt II.1.8), um den Content der Website nach den allgemeinen Themeninteressen anzupassen. Da die Auswertung anonymisiert durchgeführt werde, könne mit Hilfe des Tools der Content nicht an den konkreten Websiteuser angepasst werden. Auf Basis der Websitenutzung und Artikel-Aufrufe anonymer User erhalte die MB eine aggregierte statistische Auswertung.

Da für die allgemeine Nutzerstatistik und den bereits ausgeführten Zweck kein Personenbezug erforderlich sei, habe die MB sich bewusst zu der Einbettung der anonymisierten Variante entschlossen. Aus dem nach wie vor eingebetteten Code sei ersichtlich, dass die Funktion „anonymizeIp“ auf „true“ gesetzt worden sei. Daher verarbeite das Tool lediglich anonyme Daten. Dabei würden bei Nutzer-IP-Adressen vom Typ IPv4 das letzte Oktett und bei IPV6-Adressen die letzten 80 der 128 Bits im Speicher auf null gesetzt werden. Damit finde noch vor Speicherung oder Übermittlung der Daten eine Anonymisierung statt. Daher sei ein Zugriff auf personenbezogene Daten durch die BF2 in den Vereinigten Staaten demnach nicht möglich.

Neben anonymisierte IP-Adressen verarbeite das Tool den User Agent String. Der User Agent String diene dazu, dem Server mitzuteilen, mit welcher Systemspezifikation der User auf den Server zugreife. Dabei würden ohne Personenbezug nur das Gerät, das Betriebssystem, die Betriebssystem Version, der Browser, die Browser Version und der Gerätetyp angezeigt werden. Da diese Informationen mangels personenbezogener IP-Adresse oder sonstigem Identifer keinem bestimmbaren User zuordenbar seien, würden keine personenbezogenen Daten vorliegen. Da die Anonymisierung bereits im Arbeitsspeicher des jeweiligen Webseitenbenutzers stattfinde, erfolge keine Verarbeitung auf Servern der BF2 und sohin nicht in einem Drittland außerhalb der EU.

Noch bevor das Cookie final gesetzt werde, finde der Anonymisierungsvorgang der IP-Adresse statt. Erst ab diesem Zeitpunkt würden die statistischen Informationen rund um die Websitenutzung über den jeweiligen – nun anonymisierten – Cookie erhoben werden. Die erhobenen Auswertungen würden dementsprechend erst mit den anonymen Daten durchgeführt werden und könnten daher gar keiner Person zugeordnet werden. Auf den dargestellten Vorgang – nämlich die Erhebung und die Auswertung von bloß anonymen Daten und Informationen – fänden mangels Personenbezug weder die DSGVO noch DSG Anwendung. Demnach sei eine Einwilligung eines Websitenutzers nicht erforderlich.

Der konkrete Anonymisierungsvorgang greife initial auf die IP-Adresse zu, um diese sofort zu anonymisieren. Diese erforderliche erstmalige Erfassung der IP-Adresse erfolge jedoch unabhängig vom Einsatz von XXXX -Analytics und sei auch abseits davon stets für die Funktionsweise zwingend erforderlich. Diese Erhebung erfolge nicht zum Zwecke der MB (siehe Punkt II.1.8), sondern zwangsläufig bei jeder im Internet aufrufbaren Website. Dieser erfolge somit, wie bei jeder anderen Website auch, aufgrund von berechtigten Interesse am Betrieb einer funktionierenden, benutzerfreundlichen und sicheren Website nach Art. 6 Abs. 1 lit. f DSGVO.

Die BF2 verarbeite die Daten im Auftrag und auf Weisung der MB. Die MB nehme die Rolle des Verantwortlichen, die BF2 nehme die Rolle des Auftragsverarbeiters wahr. Die MB habe weitgehende Entscheidungsmacht über die Mittel der Verarbeitung. Sie entscheide initial darüber, ob sie das Tool überhaupt einbetten wolle und sie habe auch die Möglichkeit, die Einstellungen des Tools an die Bedürfnisse und die Zwecke der Verarbeitung zu bestimmen oder nach Bedarf zu ändern. Ferner bestimme die MB die Speicherdauer (26 Monate) sowie das Schicksal der Daten nach Vertragsbeendigung. Zu Absicherung etwaiger zukünftiger, derzeit gerade nicht stattfindenden, Übermittlungen personenbezogener Daten habe die MB daher eine Auftragsdatenverarbeitungsvereinbarung mit der BF2 abgeschlossen (siehe VWA ./16).

Nach dem Urteil des Europäischen Gerichtshofes vom 16.07.2020, C-311/18 (*Schrems II*) habe die MB die Einstellungen des Tools überprüft und sich versichert, dass die bisher datenschutzfreundliche Implementierung durch Anonymisierung der IP-Adressen weiterhin aktiv sei. Daher sei das Urteil des EuGHs nicht auf das Vertragsverhältnis zwischen der MB und der BF2 anwendbar. Um jedoch auch für eine etwaige Überlassung von personenbezogenen Daten an die BF2 Vorkehrungen zu treffen, habe die MB mit der BF2 vorsorglich eine Auftragsverarbeitervereinbarung am 12.08.2020 abgeschlossen (siehe VWA ./16) und Standardschutzklauseln einbezogen (siehe VWA ./22). Hinsichtlich der Standardschutzklauseln habe die MB keine proaktive Überprüfung vorgenommen. Dies deshalb, weil aufgrund der Übermittlung von anonymisierten IP-Adressen eine Übermittlung von personenbezogenen Daten nicht erfolge. Schließlich ergäben sich aus der Verarbeitung von anonymen Daten, die in der Folge nur für allgemeine Statistiken ausgewertet werden, keine Risiken.

Auch habe die BF2 weitere technische und organisatorische Maßnahmen gesetzt (keine Backdoor-Zugriffe für Behörden, Informationspflichten der BF2 gegenüber Verantwortlichen, wenn ein Ersuchen einer zuständigen Behörde eintrifft, Veröffentlichung von Transparenzberichten, Prüfung von Auskunftsersuchen und Rechtsmittel), um ein hohes Datenschutzniveau für die über das Tool verarbeitete Daten zu bieten.

Ihrer Stellungnahme (VWA ./11) an die bB legte die MB Berichte aus dem Tool (VWA ./12, siehe Punkt II.2), Informationen zur IP-Anonymisierung (VWA ./13, siehe Punkt II.2), Screenshot zur eingestellten Speicherdauer (VWA ./14, siehe Punkt II.2), Liste der Serverstandorte (VWA ./15, siehe Punkt II.2), Auftragsdatenverarbeitungsbedingungen für XXXX Werbeprodukte, Version 16.08.2020 (VWA ./16, siehe Punkt II.2), Auftragsdatenverarbeitungsbedingungen für XXXX Werbeprodukte, Version 12.08.2020 (VWA ./17, siehe Punkt II.2), Auftragsdatenverarbeitungsbedingungen für XXXX

Werbeprodukte, Version 01.01.2020 (VWA ./18, siehe Punkt II.2), Vergleichsversion AVV vom 01.01.2020 vs 12.08.2020 (VWA ./19, siehe Punkt II.2), Vergleichsversion AVV vom 12.08.2020 vs 16.08.2020 (VWA ./20, siehe Punkt II.2), Screenshot zu Einstellungen (VWA ./21, siehe Punkt II.2), Standarddatenschutzklauseln (VWA ./22, siehe Punkt II.2), Informationen zu Sicherheitsmaßnahmen (VWA ./23, siehe Punkt II.2) und ein Verarbeitungsblatt zu XXXX Analytics (VWA ./24, siehe Punkt II.2) bei.

I.4. Nach Aufforderung der bB vom 22.01.2021 (VWA ./25, siehe Punkt II.2) gab der BF1 in der Folge eine Stellungnahme (VWA ./26, siehe Punkt II.2) ab. Darin erklärte er, obwohl im Code die Funktion „anonymizeIP“ auf „true“ gesetzt worden sei, dies nicht zur Folge habe, dass eine anonymisierte IP-Adresse übermittelt worden sei. Dies sei bei Datentransfers im World Wide Web technisch unmöglich. Unter Verweis auf Ausführungen der BF2 führte der BF1 aus, dass die IP-Adresse erst nachdem sie im Analytics-Datenerfassungsnetzwerk eingehen, anonymisiert oder maskiert werde, bevor sie gespeichert oder verarbeitet werden würden. Zudem verwies der BF1 darauf, dass er zum Zeitpunkt des Website-Besuches in sein privates XXXX -Konto eingeloggt gewesen sei und auch Cookie-Daten (_ga, __gads, _gid, _gat, _gat_UA-259349-11, _gat_UA-259349-1) übertragen worden seien. Im Ergebnis sei also entgegen den Ausführungen der MB, klar, dass personenbezogenen Daten (wie Cookies und IP-Adressen) verarbeitet und an die BF2 in die Vereinigten Staaten übermittelt worden seien. Zudem seien bei einem Auftragsverarbeiter in einem Drittland ein Bruch der Anonymisierung nicht durchsetzbar oder feststellbar. Anhand der Sender-IP-Adresse sei im Lichte der Judikatur des Europäischen Gerichtshofes (EuGH 19.10.2016, C-582/14 *(Breyer)*) jedenfalls von einer Zuordenbarkeit zu einer bestimmten natürlichen Person auszugehen.

Um eine Verletzung der Art. 44 ff DSGVO zu verhindern, sei eine gänzliche Entfernung des Tools notwendig und ein Wechsel zu einem anderen Tool, das keine Datenübermittlung in die USA verlange, zu empfehlen. Soweit die MB der Überzeugung sei, dass keine personenbezogenen Daten verarbeitet werden würden, sei ein Abschluss von Auftragsverarbeitungsbedingungen widersinnig. Auch der Umstand, dass die MB sicherheitshalber Standarddatenschutzklauseln mit der BF2 abschließe, deute darauf hin, dass sie selbst davon ausgehe, dass eine Datenübermittlung in die USA stattfinde. Auch das von der MB vorgelegte Verarbeitungsverzeichnis (VWA ./24) deute darauf hin, dass personenbezogene Daten an die BF2 übermittelt werden würden.

Entgegen den Ausführungen der MB sei der alleinige Zweck der Erhebung der IP-Adresse nicht die Durchführung der Übertragung einer Nachricht über ein Kommunikationsnetzwerk, vielmehr werde sie auch zur Verwendung von XXXX -Analytics erhoben. Infolge möglicher Datenabgriffe durch US-Geheimdienste sei weiter davon auszugehen, dass Interessen bzw.

Grundrechte und Grundfreiheiten der betroffenen Personen, die den Schutz personenbezogener Daten erfordern, überwiegen. Wie der Europäische Gerichtshof ausgeführt habe, sei das bestehende System der Zugriffsmöglichkeiten von US-Geheimdiensten auf personenbezogene Daten von EU-Bürgern mit Art. 7, 8 und 47 GRC unvereinbar (EuGH 16.07.2020, C-311/18 (*Schrems II*)).

Seiner Stellungnahme (VWA ./26) legte der BF1 die Beilagen Drittpartner im Cookiebanner der MB (VWA ./27, siehe Punkt II.2), Kontakte von XXXX mit US-Server (VWA ./28, siehe Punkt II.2), und Kontakte von XXXX mit US-Server, Hinweis auf Fingerprinttechnologie (VWA ./29, siehe Punkt II.2) bei.

I.5. Mit Schreiben vom 26.02.2021 forderte die bB die BF2 zur Stellungnahme auf (VWA ./30, siehe Punkt II.2). Mit Eingabe vom 09.04.2021 kam die BF2 dieser Aufforderung nach (VWA ./31, siehe Punkt II.2). In ihrer Stellungnahme beschreibt die BF2 unter anderem den Webanalysedienst XXXX -Analytics (siehe Punkt II.1.3.3), die Implementierung und die Funktionsweise von XXXX -Analytics (siehe Punkt II.1.5), die Einbettung des Programmcodes für XXXX -Analytics auf einer Website (siehe Punkt II.1.6), die Rechtsgrundlage für die Nutzung von XXXX -Analytics (siehe Punkt II.1.7), die Maßnahmen, welche nach dem Urteil des Europäischen Gerichtshofes vom 16.07.2020 in der Rechtssache C-311/18 gesetzt wurden (siehe Punkt II.1.9), die ergänzenden Maßnahmen, die mit Einführung der Standardvertragsklauseln gesetzt wurden (siehe Punkt II.1.10) sowie die Auswirkungen, wenn ein Nutzer eines XXXX -Kontos eine Website besucht, welche XXXX -Analytics verwendet.

I.6. Die Eingabe der BF2 (VWA ./32) übermittelte die bB im Rahmen des Parteiengehörs der MB und dem BF1 zur Stellungnahme.

I.7. Mit Stellungahme vom 04.05.2021 (VWA ./33, siehe Punkt II.2) führte die MB aus, dass sie lediglich die kostenlose Version von XXXX Analytics verwende. Dabei sei sowohl den Auftragsdatenverarbeitungsbedingungen (Nutzungsbedingungen) als auch den Standardvertragsklauseln (SDK) zugestimmt worden. Die BF2 werde nur als Auftragsverarbeiter eingesetzt. Die Weisungen erteile die MB über die Einstellungen der XXXX -Analytics-Benutzeroberfläche und über das globale Website Tag. Es sei die Datenfreigabe-Einstellung nicht aktiviert worden. Der Code sei mit der Anonymisierungsfunktion eingebettet worden. Auch werde XXXX -Signals nicht eingesetzt. Die MB verfüge über kein eigenes Authentifizierungssystem und benutze auch keine Benutzer-ID-Funktion. Aktuell stütze man sich nicht auf die Ausnahmeregelung des Art. 49 Abs. 1 DSGVO.

I.8. Mit Stellungnahme vom 05.05.2021 (VWA ./34, siehe Punkt II.2) erklärte der BF1, dass XXXX nicht Verfahrenspartei sei und in Hinblick auf die BF2 allein Beschwerdegegenstand sei,

dass die Übermittlung und der Empfang der Daten Art. 44 ff DSGVO verfolgt sei bzw. die danach rechtswidrige Verarbeitung in den vereinigten Staaten. Gemäß Art. 44 DSGVO müssten „Verantwortliche und Auftragsverarbeiter“ die Vorgaben des Kapitel V DSGVO einhalten. Die BF2 sei als Auftragsverarbeiter Normadressat von Kapitel V DSGVO. Die bB sei für die BF2 unmittelbar zuständig, diese habe gegen Art. 44 ff DSGVO verstoßen. Hinsichtlich der von der BF2 vorgenommenen Verarbeitung sei die DSGVO anwendbar, da der sachliche Anwendungsbereich gemäß Art. 2 Abs. 1 und der räumliche Anwendungsbereich gemäß Art. 3 Abs. 2 lit. b leg.cit. erfüllt sei.

Mit Verweis auf die Stellungnahme der BF2 (VWA ./31, siehe Punkt I.5) gab der BF1 an, dass die Datenübermittlung an die BF2 in die Vereinigten Staaten sowie der Personenbezug der übermittelten Daten unbestritten sei. Die BF2 stelle außer Streit, dass alle durch XXXX -Analytics erhobenen Daten in den Vereinigten Staaten gehostet werden würden. Entsprechend den Ausführungen des BF1 würden die MB und die BF2 selbst davon ausgehen, dass es zu einer Verarbeitung personenbezogener Daten einschließlich deren Übermittlung in ein Drittland komme, da andernfalls ein Abschluss eines Auftragsdatenverarbeitungsvertrages samt Standardvertragsklauseln vollkommen sinnbefreit wäre. Auch gebe die BF2 selbst an, dass anhand einer „Benutzerkennung“ („user identifer“) eine betroffene Person zum Zwecke der Löschung identifiziert werden könne. Damit bestehe die Möglichkeit der Identifizierbarkeit im Sinne des Art. 4 Abs. 1 DSGVO. Ferner führe die BF selbst aus, dass XXXX -Analytics eindeutige Identifikationen, die mit einem bestimmten Nutzer verbunden seien verwende. Soweit die BF2 ausführe, dass die an ihr übermittelten Daten mitunter nur „pseudonyme Daten“ seien würden, so sei dies einerseits faktisch falsch und anderseits sei zu beachten, dass selbst pseudonymisierte Daten (Art. 4 Abs. 5 DSGVO) vom Begriff personenbezogene Daten gemäß Art. 4 Abs. 1 DSGVO erfasst seien.

Es sei unbestreitbar, dass die die MB und die BF2 personenbezogene Daten verarbeitet und in die Vereinigten Staaten übermittelt hätten. Zumindest einige der anlässlich des Websitebesuchs am 14. August 2020 gesetzten Cookies würden eindeutige Nutzer-Identifikations-Nummern enthalten. In der Transaktion zwischen dem Browser des BF1 und https://tracking. XXXX , die zum angeführten Datum gestartet worden sei, seien die Nutzer-Identifikations-Nummern _gads, _ga und _gid gesetzt worden. Diese Nummern seien in Folge an https://www. XXXX -analytics.com/ übermittelt worden. Es handle sich bei den Nummern um Online-Kennungen, die der Identifizierbarkeit natürlicher Personen dienten und einem Nutzer konkret zugeordnet werden würden (siehe dazu auch Punkt II.1.3). Im Hinblick auf die IP-Adresse sei festzuhalten, dass Kapitel V DSGVO keine Ausnahmen für nachträglich anonymisierte Daten vorsehe. Es sei davon auszugehen, dass die IP-Adresse des BF1 nicht

einmal in allen Transaktionen anonymisiert worden sei. Der Antrag auf Verhängung einer Geldbuße werde zurückgezogen, dies sei nunmehr eine Anregung.

Die von der BF2 vorgebrachten zusätzlichen Maßnahmen (siehe Punkt II.1.10) seien irrelevant. In diesem Zusammenhang habe der Europäische Gerichtshof folgende Elemente der US-Gesetzgebung als mit den europäischen Grundrechten gemäß Art. 7, 8 und 47 EU-Grundrechtecharta (GRC) unvereinbar gesehen (EuGH 16.07.2020, C-311/18 *(Schrems II)*, Rn 175 ff): Der Mangel jeglichen Rechtsschutzes vor US-Gerichten nach Art. 47 GRC; der Mangel jeglicher präzisen gesetzlichen Grundlage für die Überwachung, welche den Umfang und die Tragweite des Grundrechtseingriffs selbst festlegt und dem Erfordernis der Verhältnismäßigkeit genügt; der Mangel jeglicher individueller ex ante Entscheidung eines Gerichts, sondern die alleinige Überprüfung eines Überwachungssystems als Ganzes und das Fehlen jeder nachträglichen gerichtlichen Kontrolle und schließlich der Mangel jegliches Rechtsschutzes für „Nicht-US-Personen“. Vor diesem Hintergrund seien die zusätzlichen Maßnahmen (siehe Punkt II.1.10) nicht geeignet, die vom Europäischen Gerichtshof dargestellten Probleme zu lösen. Mit umfassender Begründung führte der BF1 aus, dass keine der vermeintlichen „zusätzlichen Maßnahmen“ über den normalen Standard der Datenverarbeitung gemäß Art. 32 DSGVO hinausgehe oder Relevanz in Hinblick auf Datenzugriffe der US-Regierung gemäß 50 U.S. Code § 1881a und/oder EO 12.333 habe.

Seiner Stellungnahme (VWA ./34) legte der BF1 die Beilagen „ XXXX -Analytics Cookie, Verwendung auf Website“ (VWA ./35, siehe Punkt II.2), „So verwendet XXXX Cookies“ (VWA ./36, siehe Punkt II.2), und „Measurement Protocol Parameter Reference“ (VWA ./37, siehe Punkt II.2) bei.

I.9. In Folge forderte die bB die Verfahrensparteien zur neuerlichen Stellungnahme auf (VWA ./38, ./39 und ./40, siehe Punkt II.2). Mit E-Mail vom 12.05.2021 beantragte die BF2 eine Verlängerung der Frist zur Stellungnahme (VWA ./41, siehe Punkt II.2), welche anschließend von der bB gewährt wurde (VWA ./42, siehe Punkt II.2).

I.10. In ihrer Stellungnahme vom 10.06.2021 (VWA ./43, siehe Punkt II.2) führte die BF2 aus, dass die Aktivlegitimation des BF1 nicht festgestellt worden sei, da nicht nachgewiesen worden sei, dass es sich bei den übermittelten Daten um personenbezogene Daten des BF1 handle. Um die verfahrensgegenständlichen Daten (Cookies, IP-Adresse) als personenbezogene Daten des BF1 qualifizieren zu können, müsste er auf der Grundlage dieser Daten identifizierbar seien.

Hinsichtlich der Nummern _gid und cid sei anzumerken, dass diese First-Party-Cookies seien, welche unter der Domain XXXX gesetzt worden seien. Es seien daher nicht Cookies der BF2,

sondern Cookies des Website-Besitzers, und die Cookie-Werte seien für jeden Nutzer auf jeder Website unterschiedlich. Der BF1 habe ausgeführt, dass die Nummern „_gid“ und „cid“ an https://www. XXXX -analytics.com/ übermittelt worden seien. „_gid“ habe den Wert 1284433117.1597223478 und „cid“ den Wert 929316258.1597394734. Zur Beurteilung der Aktivlegitimation müsse daher festgestellt werden, ob diese Nummern (Werte) den BF1 identifizierbar machen.

In Anbetracht der Tatsache, dass ein einzelner Nutzer unterschiedliche cid-Nummern für verschiedene Websites habe und die cid-Nummern nach dem Zufallsprinzip generiert werden, könne eine solche cid-Nummer für sich genommen einen Nutzer nicht identifizieren. Die Nummer 929316258.1597394734 identifiziere den BF1 schlichtweg nicht. Der BF1 bringe nicht vor, dass spätere Besuche der Website stattgefunden hätten, geschweige denn, dass Daten im Zusammenhang mit solchen späteren Besuchen der Website in Verbindung mit der cid 929316258.1597394734 erfasst worden wären. Es seien keine Umstände hervorgekommen, aufgrund dessen man argumentieren könnte, dass in Verbindung mit der cid-Nummer 929316258.1597394734 gesammelte Informationen den BF1 identifizierbar machen würden. Diese Ausführungen gelten im Wesentlichen auf die _gid-Nummern.

Im Hinblick auf die IP-Adresse sei zu prüfen, ob die IP-Adresse des mit dem Internet verbundenen Geräts tatsächlich dem BF1 zuzuordnen sei und ob der Verantwortliche oder eine andere Person die rechtlichen Mittel habe, um Anschlussinhaberinformationen von dem betreffenden Internetzugangsanbieter zu erhalten.

Selbst wenn festgestellt würde, dass die MB oder eine andere Person theoretisch solche rechtlichen Mittel im Sinne des Erwägungsgrundes 26 habe, um Anschlussinhaberinformationen in Bezug auf den B1 vom Internetzugangsanbieter zu erhalten, müsse weiters noch festgestellt werden, ob es im Sinne des Erwägungsgrundes 26 DSGVO nach allgemeinem Ermessen wahrscheinlich sei, dass diese Mittel genutzt werden würden. Nach allgemeinem Ermessen sei nicht wahrscheinlich, dass die MB oder eine andere Person im Sinne von Erwägungsgrund 26 rechtliche Mittel (sofern ihnen solche zur Verfügung stehen) einsetzen würde. Insbesondere in der verfahrensgegenständlichen Situation, wäre es nach allgemeinem Ermessenunwahrscheinlich, dass solche rechtlichen Mittel eingesetzt würden, um einen beliebigen Besucher einer Webseite wie den BF1 zu identifizieren, wenn man die objektiven Faktoren, wie die Kosten und den Zeitaufwand solcher Mittel für die Identifizierung (siehe Erwägungsgrund 26) berücksichtige.

Als Auftragsverarbeiter stelle die BF2 dem Website-Betreiber zahlreiche Konfigurationsmöglichkeiten von XXXX -Analytics zur Verfügung. Die Anonymisierungsfunktion sei entsprechend den Erklärungen der MB vom 16.12.2020 (VWA

./11) und 04.05.2021 (VWA ./33) konfiguriert worden. Jedoch sei aufgrund eines möglichen Konfigurationsfehlers seitens der MB die Anonymisierungsfunktion nicht in allen Fällen aktiviert worden.

Unter normalen Betriebsbedingungen und soweit Nutzer mit Sitz in der EU betroffen seien, befinde sich ein Webserver im EWR, weshalb die IP-Anonymisierung grundsätzlich innerhalb des EWR erfolge. Im vorliegenden Fall seien normale Betriebsbedingungen vorgelegen.

Am 14. August 2020 habe das XXXX -Konto des BF1 (XXXX) die Web-&-App Aktivitäten Einstellung aktiviert. Allerdings habe sich das Konto nicht entschieden, Aktivitäten von Websites einzuschließen, die XXXX -Dienste nutzten. Da die MB nach eigenen Angaben auch XXXX -Signals nicht aktiviert habe, sei die BF2 nicht in der Lage (gewesen), festzustellen, dass der Nutzer des XXXX -Kontos XXXX die XXXX besucht habe.

Im Hinblick auf den internationalen Datenverkehr sei festzuhalten, dass selbst unter der Annahme, dass es sich um personenbezogene Daten des Beschwerdeführers handle, diese ihrer Art nach im Hinblick auf Quantität und Qualität begrenzt seien. Soweit die übermittelten Daten überhaupt als personenbezogene Daten zu qualifizieren seien, würde es sich auch um pseudonyme Daten handeln.

Es seien Standardvertragsklauseln mit der MB abgeschlossen worden, zusätzlich seien ergänzende Maßnahmen implementiert worden. Die BF2 lege keine Nutzerdaten gemäß EO 12333 offen. FISA § 702 sei im vorliegenden Fall angesichts der Verschlüsselung und der Anonymisierung von IP-Adressen irrelevant.

Die Art. 44 ff DSGVO könnten nicht Gegenstand eines Beschwerdeverfahrens nach Art. 77 Abs. 1 DSGVO sein, weshalb die Beschwerde dahingehend zurückzuweisen sei.

Schließlich seien die Art. 44 ff DSGVO seien im Hinblick auf die BF2 als Datenimporteur auch nicht anwendbar.

I.11. Die Eingabe der BF2 wurde von der bB dem BF1 und der MB im Rahmen des Parteiengehörs übermittelt (VWA ./44, siehe Punkt II.2). Dahingehend beantragte der BF1 eine Verlängerung der Frist zur Stellungnahme (VWA ./45, siehe Punkt II.2). Weiters forderte die bB die MB mit Schreiben vom 16.06.2021 auf bekanntzugeben, ob es bei rechtliche Änderungen gegeben habe und die anwaltliche Vertretung nach wie vor bestehe (VWA ./46, siehe Punkt II.2).

I.12. Mit Stellungnahme vom 18.06.2021 teilte die MB die Änderung ihrer Firma und die Übertragung der Website auf eine andere juristische Person mit (siehe Punkt II.1.2, sowie VWA ./47, siehe Punkt II.2).

I.13. Mit weiterer Stellungnahme vom 18.06.2021 (VWA ./48, siehe Punkt II.2). führte die MB aus, dass die beabsichtigte IP-Anonymisierung aufgrund eines Programmierfehlers nicht aktiviert gewesen sei. Aufgrund der vorgenommenen Änderung sei nunmehr für alle XXXX -Analytics Properties auf der Website XXXX die IP-Anonymisierung aktiviert (VWA ./50, siehe Punkt II.2). In der Folge sei die BF2 angewiesen worden, alle über die XXXX -Analytics-Properties gesammelten Daten sofort zu löschen. Die BF2 habe die Löschung mittlerweile bestätigt (VWA ./49, ./52 und ./53 siehe Punkt II.2). Aufgrund der vorgenommenen Löschung verarbeite weder die MB noch die BF2 Daten des BF1. Es werde daher gemäß § 24 Abs. 6 DSG die formlose Einstellung des Verfahrens angeregt. Die Stellungnahme der MB wurde dem BF1 zur Kenntnisnahme übermittelt (VWA ./51, siehe Punkt II.2).

I.14. In der Eingabe vom 09.07.2021 (VWA ./54, siehe Punkt II.2) gab die BF2 an, dass die Angemessenheitsbeurteilung nach den *Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten, Version 2.0* des Europäischen Datenschutzausschusses („EDSA-Empfehlungen“) nicht auf die Prüfung der Rechtsvorschriften des Drittlandes beschränkt sei. Es müssen auch alle spezifischen Umstände der gegenständlichen Übermittlung berücksichtigen werden. Im vorliegenden Fall seien die verarbeiteten personenbezogenen Daten aufgrund der begrenzten Art und der geringen Sensibilität anders zu behandeln als die Daten, welche Gegenstand der Schrems-I- und Schrems-II-Urteile. Dies sei für den gegenständlichen Fall relevant. Im Ergebnis werde vom Europäischen Datenschutzausschuss ein risikopassierter Ansatz empfohlen.

Auch sie die tatsächliche Wahrscheinlichkeit eines behördlichen Zugriffs auf die Daten ein relevanter Faktor für die Angemessenheitsbeurteilung. Selbst bei Vorliegen problematischer Gesetzgebung könne eine Fortsetzung der Datenübermittlung zulässig sein (auch ohne Durchführung zusätzlicher Maßnahmen), wenn der Exporteur keinen Grund zur Annahme habe, dass die problematische Gesetzgebung in der Praxis so ausgelegt und/oder angewandt werden könnte, dass sie die übermittelten Daten und den spezifischen Datenimporteur erfassen würde. Zudem sei für die Beurteilung nicht mehr ausschließlich die Gesetzgebung des Drittlandes von Bedeutung, sondern auch die Frage, ob die Praxis dies anwende oder auch nicht. So sei aus dem White Paper *„Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Basis for EU-U.S. Data Transfers after Schrems II"* zu entnehmen, dass die meisten Unternehmen, die in der EU tätig seien, keine Daten verarbeiten, die für US-Geheimdienste von Interesse seien.

Wenn ein Datenexporteur personenbezogene Daten in einer Weise übermittle, dass die personenbezogenen Daten ohne die Kombination mit weiteren Daten nicht mehr einer

bestimmten betroffenen Person zugeordnet werden können, sei entsprechend der EDSA-Empfehlungen die durchgeführte Pseudonymisierung eine wirksame ergänzende Maßnahme. Es sei nicht zu erwarten, dass US-Behörden über zusätzliche Informationen verfügen, die es ihnen ermöglichen würde, die hinter den First Party Cookie-Werten _gid und cid bzw. hinter einer IP-Adresse stehenden betroffenen Personen zu identifizieren.

Schließlich habe der BF1 auch nicht die Feststellung beantragt, dass seine Rechte in der Vergangenheit verletzt worden seien.

I.15. In seiner Stellungnahme vom 09.07.2021 (VWA ./55, siehe Punkt II.2) erklärte der BF1, dass eine Verarbeitung von personenbezogenen Daten gegeben sei. Dies sei durch die vorgelegten Unterlagen (VWA ./5 sowie VWA ./34, Punkt 5.3) belegt worden. Auch würden Vertragsdokumente (Auftragsdatenverarbeitungsbedingungen oder Standarddatenschutzklauseln) einen Personenbezug nicht erzeugen, jedoch seien diese Dokumente ein wichtiges Indiz, dass sowohl die BF2 als auch die MB von einem Personenbezug ausgehen würden. Auch gehe die BF2 selbst von einer Identifizierbarkeit des BF1 aus. Wenn es letztlich für die Identifikation eines Website-Besuchers nur Voraussetzung sei, ob dieser eine gewisse Willenserklärungen in seinem XXXX -Konto abgebe (wie etwa die Aktivierung von „Ad personalisation“), würden für die BF2 alle Möglichkeiten der Identifizierbarkeit vorliegen. Andernfalls könne die BF2 den in den Kontoeinstellungen ausgedrückten Wünschen eines Nutzers nach „Personalisierung“ der erhaltenen Werbeinformationen nicht entsprechen.

Der UUID (Universally Unique Identifier) im _gid-Cookie mit dem UNIX-Zeitstempel 1597223478 sei am Mittwoch, 12 August 2020 um 11:11 und 18 Sekunden MEZ gesetzt worden, jene im cid-Cookie mit dem UNIX-Zeitstempel 1597394734 am Freitag, 14. August 2020 um 10:45 und 34 Sekunden MEZ. Daraus folge, dass diese Cookies schon vor dem beschwerdegegenständlichen Besuch verwendet worden seien und auch ein längerfristiges Tracking stattgefunden habe. Der BF1 habe seines Wissens diese Cookies auch nicht unmittelbar gelöscht und die Webseite XXXX auch wiederholt besucht.

Die BF2 verkenne das weite Verständnis der DSGVO bei der Beurteilung des Vorliegens personenbezogener Daten. Die konkret genutzte IP-Adresse sei auch für den BF1 nicht mehr feststellbar. Dies sei aber irrelevant, da über die UUID in den Cookies ohnehin ein klarer Personenbezug bestehe. Speziell die Kombination von Cookie-Daten und IP-Adresse erlaube Tracking und die Auswertung von geografischer Lokalisation, Internet-Anschluss und Kontext des Besuchers, die mit den bereits beschriebenen Cookie-Daten verknüpfbar seien. Hierzu würden aber auch Daten wie der genutzte Browser, die Bildschirmauflösung oder das Betriebssystem („Device Fingerprinting“) kommen.

Im Rahmen der Beschwerde relevanter sei, dass US-Behörden gerade für Geheimdienste leicht feststellbare Daten, wie etwa die IP-Adresse, als Ausgangspunkt für die Überwachung von Einzelpersonen nutzen würden. Es sei das Standardvorgehen von Geheimdiensten, sich von einem Datum zu anderen „weiterzuhangeln“. Wenn der Computer des BF1 etwa immer wiederüber die IP-Adresse von XXXX im Internet auftauche, so könne dies genutzt werden, um die Arbeit des Vereins XXXX auszuspähen und um den BF1 ins Visier zu nehmen. In einem weiteren Schritt würden dann andere Identifier in den Daten gesucht, wie etwa die genannten UUIDs, was wiederrum eine Identifikation der einzelnen Person für eine Überwachung an anderen Orten ermögliche. Bei US-Geheimdiensten handle es sich in diesem Zusammenhang sohin um eine „andere Person“ im Sinne des Erwägungsgrundes 26 DSGVO. Der BF1 arbeite nicht nur für XXXX , sondern habe als Musterbeschwerdeführer auch eine relevante Rolle in diesen Anstrengungen. Damit sei nach US-Recht eine Überwachung des BF1 nach 50 USC § 1881a (ebenso wie von allen anderen mit dieser Beschwerde betrauten Personen) jederzeit legal möglich. Selbst bei der Anwendung des vermeintlichen „risikobasierten Ansatzes“ sei der gegenständliche Fall ein Paradebeispiel für ein hohes Risiko.

Die E-Mail-Adresse XXXX sei dem BF1 zuzuordnen, der bis zu seiner Eheschließung den Nachnamen “ XXXX “ getragen habe. Das alte XXXX -Konto werde jedoch noch immer benutzt. Die BF2 habe nicht erklärt, inwieweit die unstrittig vorliegenden Daten verknüpft, ausgewertet oder das Ergebnis einer Auswertung dem Nutzer nur nicht angezeigt werde.

Darüber hinaus kenne Kapitel V DSGVO keinen „risikobasierten Ansatz“. Dieser finde sich nur in bestimmten Artikeln der DSGVO, wie etwa in Art. 32 leg.cit. Die neuen Standardvertragsklauseln im Durchführungsbeschluss (EU) 2021/914 seien für den Sachverhalt mangels zeitlicher Gültigkeit nicht relevant. Eine „Übermittlung“ sei keine einseitige Handlung eines Datenexporteurs, jede „Übermittlung“ verlange auch einen Empfang der Daten. Demnach sei das Kapitel V der DSGVO auch für die BF2 anwendbar, es handle sich um ein gemeinschaftliches Handeln von Datenexporteur und -importeur.

Sofern der BF2 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 die BF2 einer entsprechenden Weisung eines US-Geheimdienstes Folge, so treffe er damit die Entscheidung, personenbezogene Daten über den konkreten Auftrag der MB gemäß Art. 28 und Art. 29 DSGVO und den entsprechenden Vertragsdokumenten hinaus zu verarbeiten. Hierdurch werde die BF2 gemäß Art. 28 Abs. 10 DSGVO selbst zum Verantwortlichen. Infolgedessen habe die BF2 insbesondere auch die Bestimmungen der Art. 5 ff DSGVO zu befolgen. Eine heimliche Datenweitergabe an US-Geheimdienste gemäß dem Recht der USA

sei ohne Zweifel nicht mit Art. 5 Abs. 1 lit. f DSGVO, Art. 5 Abs. 1 lit. a DSGVO und Art. 6 DSGVO vereinbar.

I.16. Nach Aufforderung zur Stellungnahme (VWA ./56, siehe Punkt II.2) führte die BF2 mit ihrer Eingabe vom 12.08.2021 (VWA ./57, siehe Punkt II.2) aus, dass der BF1 seine Aktivlegitimation zur Beschwerdeeinbringung nicht dargetan habe. Er habe keine seitens der BF2 aufgeworfenen Fragen zur Identifizierbarkeit seiner Person anhand der IP-Adresse beantwortet. In Bezug auf die _gid-Nummer und cid-Nummer sei festzuhalten, dass kein Verzeichnis vorhanden sei, um dadurch den BF2 identifizierbar zu machen. Die Tatsache, dass in ErwGr 26 DSGVO das „Aussondern" als mögliches Mittel zur Identifizierung erwähnt sei, ändere jedoch nicht das Verständnis der Worte „identifizieren" oder „Identifizierung" oder „Identifizierbarkeit".

Die Identifizierbarkeit des BF1 setze zumindest voraus, dass seine Identifizierung auf Grundlage der gegenständlichen Daten und mit Mitteln möglich sei, die nach allgemeinem Ermessen wahrscheinlich genutzt würden. Dies sei nicht festgestellt und könne nicht unterstellt werden und sei im Gegenteil sogar unwahrscheinlich, wenn nicht sogar unmöglich. Auch die Tatsache, dass die BF2 Auftragsdatenverarbeitungsbedingungen abgeschlossen habe, bedeute weder, dass es sich bei den Daten, die Gegenstand dieses Verfahrens seien, um personenbezogene Daten handle, noch, dass es sich um die Daten des BF1 handle.

Der Ansicht des BF1, dass die Datenübermittlung nicht nach einem risikobasierten Ansatz zu bewerten sei („Alles-oder-Nichts"), sei nicht zu folgen. Dies stehe nicht im Einklang mit der DSGVO und sei an ErwGr 20 des Durchführungsbeschlusses (EU) 2021/914 der Europäischen Kommission zu sehen. Ebenso sei dies an den unterschiedlichen Versionen der EDSA-Empfehlung erkennbar. Selbst wenn ein Zugriff auf die oben angeführten Nummern durch US-Behörden „jederzeit legal" möglich sei, sei zu überprüfen, wie wahrscheinlich dies sei. Der BF1 habe keine überzeugenden Argumente dafür vorgebracht, warum oder wie die „Cookie-Daten" im Zusammenhang mit seinem Besuch einer öffentlich zugänglichen, und von vielen genutzten österreichischen Website wie der in Rede stehenden, „Foreign Intelligence Information" seien und damit zum Ziel der zweckbeschränkten Datenerfassung gemäß § 702 werden könnten.

I.17. Mit verfahrensgegenständlichen Bescheid (VWA ./59, siehe Punkt II.2) behob die bB mit Spruchpunkt 1. zunächst den Bescheid vom 02.10.2020, Zl 2020-0.527.385 (DSB-D155.027) (siehe Punkt I.2).

Mit Spruchpunkt 2. gab die bB der Beschwerde gegen die MB statt und stellte fest, dass (a) die MB als Verantwortliche durch Implementierung des Tools „ XXXX -Analytics" auf ihrer

Website unter XXXX zumindest am 14. August 2020 personenbezogene Daten des BF1 (dies sind zumindest einzigartige Nutzer-Identifikations-Nummern, IP-Adresse und Browserparameter) an die BF2 übermittelt habe, (b) die Standarddatenschutzklauseln, die die MB mit der BF2 abgeschlossen habe, kein angemessenes Schutzniveau gemäß Art. 44 DSGVO bieten würden, da (i) die BF2 als Anbieter elektronischer Kommunikationsdienste im Sinne von 50 U.S. Code § 1881(b)(4) zu qualifizieren sei und als solcher der Überwachung durch US-Geheimdienste gemäß 50 U.S. Code § 1881a („FISA 702“) unterliege, und (ii) die Maßnahmen, die zusätzlich zu den in Spruchpunkt 2. b) genannten Standarddatenschutzklauseln getroffenen worden seien, nicht effektiv seien, da diese die Überwachungs- und Zugriffsmöglichkeiten durch US-Nachrichtendienste nicht beseitigen würden und (c) im vorliegenden Fall kein anderes Instrument gemäß Kapitel V der DSGVO für die in Spruchpunkt (2.a) angeführte Datenübermittlung herangezogen werden könne und die MB deshalb für die im Rahmen der in Spruchpunkt 2.a) angeführte Datenübermittlung kein angemessenes Schutzniveau gemäß Art. 44 DSGVO gewährleistet habe.

Mit Spruchpunkt 3. wies die bB die Beschwerde wegen einer Verletzung der allgemeinen Grundsätze der Datenübermittlung gemäß Art. 44 DSGVO gegen die BF2 ab.

In ihrer rechtlichen Begründung setzt sich die bB zunächst mit ihrer Zuständigkeit und ihrer Feststellungkompetenz (siehe dazu Punkt II.3.4) auseinander. Auch beschreibt sie, dass Art. 44 DSGVO als subjektives Recht zu werten sei (siehe dazu Punkt II.3.4). Im Zusammenhang mit Spruchpunkt 2. führte die bB aus, dass die übermittelten Daten (siehe Punkt II.1.3 bzw. II.1.3.1) jedenfalls in Kombination personenbezogene Daten gemäß Art. 4 Z 1 DSGVO seien. Zum fehlenden angemessenen Schutzniveau gemäß Art. 44 DSGVO gab die bB an, dass der Europäische Gerichtshof das „EU-US Privacy Shield“ mit der Entscheidung vom 16.07.2020, C-311/18 *(Schrems II)* für ungültig erklärt habe. Auch könne die verfahrensgegenständliche Datenübertragung nicht allein auf die zwischen der MB und der BF2 abgeschlossenen Standarddatenschutzklauseln gemäß Art. 46 Abs. 2 lit. c DSGVO gestützt werden. Auch seien die von der BF2 aufgezeigten zusätzlichen Maßnahmen nicht geeignet, die im Urteil aufgezeigten Rechtsschutzlücken – unangemessene Zugriffs- und Überwachungsmöglichkeiten von US-Nachrichtendiensten sowie unzureichender wirksamer Rechtsbehelf für Betroffene – zu schließen.

Die Abweisung im Spruchpunkt 3. begründete die bB damit, dass die Voraussetzungen des Art. 44 DSGVO auf die BF2 nicht zutreffen würden. Die BF2 lege die personenbezogenen Daten des BF1 nicht offen, sondern erhalte sie nur. Die Vorgaben von Kapitel V DSGVO seien vom Datenexporteur und nicht auch von einem Datenimporteur (in einem Drittstaat) einzuhalten.

Der Bescheid wurde dem BF1 am 12.01.2022, der BF2 und der MB am 13.01. zugestellt. Gegen den Spruchpunkt 3. des Bescheides erhob der BF1 am 07.02.2022 eine Bescheidbeschwerde (siehe Punkt I.20). Die BF2 erhob am 09.02.2022 gegen Spruchpunkt 2. des Bescheides eine Bescheidbeschwerde (siehe Punkt I.17I.18). Seitens der MB erfolgte keine Bescheidbeschwerde. Verfahren gg Websitenbetreiber ist daher abgeschlossen!

I.18. In ihrer Bescheidbeschwerde (VWA ./62, siehe Punkt II.2) begründete die BF2 zunächst ihre Beschwerdelegitimation. Ferner führte die BF2 aus, dass zwischen dem Gegenstand des angefochtenen Teilbescheides und dem Gegenstand des in Aussicht genommenen zweiten Teilbescheides keine Trennbarkeit gemäß § 59 Abs. 1 AVG bestehe. Auch liege eine Verletzung eines Betroffenenrechts nicht vor. Zudem könne eine Feststellung angeblicher, in der Vergangenheit liegender, Verletzungen nicht vorgenommen werden. Auch liege eine Verbandsklagebefugnis nach Art. 80 Abs. 2 DSGVO nicht vor.

Entgegen der Ansicht der bB seien die verfahrensgegenständlichen Daten nicht personenbezogen i.S.d. DSGVO. Begründend führte die BF2 aus, dass sich aus den verarbeiteten Daten kein Bezug zu einer natürlichen Person ergebe. Entsprechend der Rechtsprechung des Europäischen Gerichtshofes (EuGH 20.12.2017, C-434/16 *(Nowak)*, Rn 35) liege weder ein Inhaltselement, ein Zweckelement noch ein Ergebniselement vor. Ferner sei keine Identifizierbarkeit einer natürlichen Person gegeben. Aus der spezifizierten IP-Adresse, den XXXX -spezifischen Zufallszahlen, den Browserparametern und den seiten-bezogenen Daten lasse sich eine bestimmte Person nicht identifizieren. Auch aus einer Kombination dieser Daten sei eine Identifizierung nicht möglich. Weiters habe die BF2 keine technischen Möglichkeiten, den BF1 über sein XXXX -Konto zu identifizieren.

Ferner betonte die BF2 einen risikobasierten Ansatz. Auch wenn man den verfahrensgegenständlichen Daten einen Personenbezug unterstelle, so sei unter Berücksichtigung der Niederschwelligkeit der übermittelten Daten und dem damit sehr geringen Basisrisiko, der Unanwendbarkeit von und des Umstandes, dass FISA 702 ohnehin keine praktische Anwendung finde, keine Offenlegung von Daten gemäß EO 12.333 erfolgt. Da umfangreiche ergänzende Maßnahmen implementiert worden seien, sei ein angemessenes Schutzniveau für die verfahrensgegenständliche Übermittlung der Daten mehr als gegeben und diese nach Art. 44 ff DSGVO zulässig.

Ihrer Bescheidbeschwerde legte die BF2 die Beilagen Cookies und User Identification (VWA ./63, siehe Punkt II.2), Linker (VWA ./64, siehe Punkt II.2), Report von XXXX (VWA ./65, siehe Punkt II.2) und New EU-US data trasfer framework (VWA ./66, siehe Punkt II.2) bei.

I.19. Zur Bescheidbeschwerde der BF2 führte die bB in der Stellungnahme (VWA ./67, siehe Punkt II.2) im Zuge der Aktenvorlage aus, dass die BF2 keine Beschwerdelegitimation habe, da seit Ende April 2021 das Produkt XXXX -Analytics nunmehr von XXXX angeboten werde. Auch erklärte die bB, dass ihr eine Feststellungskompetenz in Beschwerdeverfahren wegen behaupteten Verstößen gegen das DSG oder gegen die DSGVO zukomme.

Weiters gab die bB an, dass die BF2 offenkundig selbst von einer Vereinbarung personenbezogener Daten ausgehe. Dies erkenne man daran, dass die BF2 mit der MB unstrittig eine Auftragsverarbeitervereinbarung gemäß Art. 28 Abs. 2 DSGVO sowie eine Standarddatenschutzklausel gemäß Art. 46 Abs. 2 lit. c DSGVO abgeschlossen habe. Auch habe die BF2 ausgeführt, dass ein Website-Betreiber in allen Fällen Standarddatenschutzklauseln mit der BF2 abschließe (VWA ./31, Seite 3). Auch deklariere die BF2 selbst, dass Online-Kennzeichnungen personenbezogene Daten seien (siehe Punkt II.1.3.6). Unabhängig von diesen Erklärungen bzw. Verhaltensweisen der BF2 würden verfahrensgegenständlich unter Berücksichtigung der Judikatur des Europäischen Gerichtshofes und Erklärungen des Europäischen Datenschutzbeauftragten (VWA ./68) personenbezogene Daten vorliegen. Auch könne im vorliegenden Fall eine Zuordnung über die IP-Adresse vorgenommen werden. Zudem könne auch mit Browserinformationen eine Kombination vorgenommen werden. In diesem Zusammenhang verwies die bB auf die Definition von „Fingerprinting“: Dies sei ein Vorgang, bei dem ein Beobachter ein Gerät oder eine Anwendungsinstanz mit ausreichender Wahrscheinlichkeit auf Grundlage mehrerer Informationselemente identifizieren könne.

Schließlich widerlegte die bB ausführlich den aufgezeigten risikobasierten Ansatz der BF2 und wies darauf hin, dass wirtschaftliche Interessen keine Rolle bei der Entscheidung des Europäischen Gerichtshofes am 16.07.2020, C-311/18 (*Schrems II*) spielten.

Seiner Stellungnahme legte die bB eine Entscheidung des Europäischen Datenschutzbeauftragten vom 05.01.2022 (VWA ./68, siehe Punkt II.2), eine Entscheidung des LG München (VWA ./69, siehe Punkt II.2), ein Gutachten zum aktuellen Stand des US-Überwachungsrechts (VWA ./70, siehe Punkt II.2) sowie wesentliche Befund des Gutachtens zum aktuellen Stand des US-Überwachungsrechts (VWA ./71, siehe Punkt II.2) bei.

I.20. In seiner Bescheidbeschwerde (VWA ./60, siehe Punkt II.2) führte der BF1 aus, dass die bB die Abweisung in Spruchpunkt 3. mit einer verfehlten Wortinterpretation des Art. 44 DSGVO begründe. Soweit die bB ihre Abweisung damit begründe, dass die BF2 als Empfänger der personenbezogenen Daten im Drittland Vereinigte Staaten (Datenimporteur) die Daten nicht offenlege, sondern sie (nur) erhalte, verkenne die bB, dass Art. 44 DSGVO den Begriff „Offenlegung“ nicht verwende. Art. 44 DSGVO verwende den Begriff „Übermittlung“. Die Unterscheidung zwischen diesen Begriffen sei gegenständlich entscheidend: Im Gegensatz zu

einer „Offenlegung“, die auch ohne einen designierten Empfänger geschehen könne (etwa durch Veröffentlichung auf einer Website) benötige eine „Übermittlung“ (bzw. eine „Offenlegung durch Übermittlung“) nämlich stets einen Empfänger und auch dessen (zumindest minimales) Zutun. Während eine „Offenlegung“ mit dem Akt des „Verfügbarmachens“ abgeschlossen sei, verlange eine „Übermittlung“ auch eine Entgegennahme durch den Empfänger.

In juristischer Hinsicht verdeutliche die Gestaltung von Kapitel V DSGVO die technische Realität (gemeint, dass für die Übertragung im Internet stets ein Zusammenwirken eines Senders und eines Empfängers erforderlich ist). Bereits Art. 44 DSGVO verlange generell von „Verantwortlichem und der Auftragsverarbeiter“ die Einhaltung der Bestimmungen des Kapitels, ohne dies auf den „die Daten exportierenden Verantwortlichen oder Auftragsverarbeiter“ zu beschränken. Auch die in Art. 46(2) DSGVO genannten Garantien verlangen durchwegs ein Zusammenwirken von Datenexporteur und Datenimporteur und beinhalten insbesondere auch Verpflichtungen des Datenimporteurs. Richtigerweise seien auch hier sowohl der Datenexporteur, als auch der Datenimporteur zur Befolgung der genannten Bestimmungen verpflichtet, da sie gemeinsam Daten aus der EU hinaus in das Drittland und vom Drittland in die EU übermitteln würden.

Zudem sei zu beachten, dass auch Verpflichtungen aus den Standardvertragsklauseln *(Durchführungsbeschluss 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)* für den Datenimporteur zu entnehmen seien. Klausel 3(2) enthalte eindeutig eine subsidiäre Verpflichtung des Datenimporteurs, die Klauseln 5(a) bis (e), 6, 7, 8(2) und 9 bis 12 der Standardvertragsklauseln der betroffenen Person gegenüber zu befolgen, wenn das Unternehmen des Datenexporteurs faktisch oder rechtlich nicht mehr bestehe und kein Rechtsnachfolger die Pflichten des Datenexporteurs übernommen habe. Wäre Kapitel V DSGVO nicht auch auf den Datenimporteur anwendbar, wäre die Durchsetzung der subjektiven Rechte der betroffenen Person aus den Standardvertragsklauseln gegenüber dem Datenimporteur unmöglich.

I.21. Zur Bescheidbeschwerde des BF1 führte die bB in der Stellungnahme (VWA ./61, siehe Punkt II.2) im Zuge der Aktenvorlage aus, dass es aus technischer Sicht korrekt sei, dass eine Übermittlung (anders als eine Offenlegung an einen unbestimmten Adressatenkreis, etwa in Form einer Veröffentlichung auf einer Website) voraussetze, dass es einen Empfänger gäbe. Wie jedoch bereits im angefochtenen Bescheid ausgeführt sei, können sich bei einem Verarbeitungsvorgang (hier also bei der „Übermittlung“) aus rechtlicher Sicht unterschiedliche

Pflichten und Grade der Verantwortung ergeben (VWA ./59, Seite 40). In Einklang mit den „Leitlinien 5/2021 des EDSA zum Verhältnis zwischen dem Anwendungsbereich von Art. 3 und den Vorgaben für den Internationalen Datenverkehr gemäß Kapitel V DSGVO“ gehe die bB davon aus, dass den Datenimporteur nicht die rechtliche Verpflichtung treffe, die Vorgaben von Art. 44 DSGVO einzuhalten.

Schließlich sei festzuhalten, dass dem Datenimporteur selbstverständlich auch entsprechende Pflichten treffen würden. Im Falle des Abschlusses von Standardvertragsklauseln nach Art. 46 Abs. 2 lit. c DSGVO habe ein Datenimporteur sämtliche vertraglichen Verpflichtungen einzuhalten, die zwischen diesem und seinem Vertragspartner abgeschlossen worden seien. Diese Verpflichtungen seien aber vertraglicher Natur. Hingegen habe (nur) der Datenexporteur die Verpflichtungen aus Art. 44 DSGVO einzuhalten, wozu auch zähle, dass ein passendes Instrument – wie etwa der Abschluss von Standardvertragsklauseln – vorhanden sei, um ein angemessenes Schutzniveau zu gewährleisten.

I.22. Mit Eingabe vom 08.07.2022 übermittelte die BF2 eine Replik zur Bescheidbeschwerde des BF1 (OZ 4 zu W245 2252208-1). Darin begründete die BF2 ausführlich, dass Art. 44 ff DSGVO nicht auf XXXX als Datenimporteurin anwendbar sei.

I.23. In seiner Stellungnahme vom 13.01.2022 (OZ 4 zu W245 2252208-1) verwies der BF2 wiederholt darauf hin, dass verfahrensgegenständlich personenbezogene Daten verarbeitet worden seien. Zudem führte der BF2 aus, dass aus Art. 44 ff DSGVO ein risikobasierter Ansatz nicht zu entnehmen sei. Ferner führte der BF2 mit näherer Begründung aus, dass auch die BF1 als Datenimporteuer von Kapitel V DSGVO unmittelbar erfasst sei.

I.24. Mit Stellungnahme vom 14.02.2023 (OZ 15 zu W245 2252208-1) führte die BF2 aus, dass aufgrund der spruchmäßigen Feststellungen eine Bindungswirkung bestehe. Insbesondere, dass im Spruch festgestellt worden sei, dass personenbezogene Daten übertragen worden seien, habe evidente Auswirkungen auf weitere Verfahren bei der bB zur Folge. Die BF2 könne diesen Umstand in den weiteren Verfahren nicht wiederlegen.

Zum Personenbezug führte die BF2 wiederholend aus, dass dieser nicht vorliege. Dazu wurden auch zwei eidesstattliche Erklärungen vorgebracht, die belegen sollen, dass die BF2 nicht in der Lage gewesen sei, über das XXXX -Konto des BF1 einen Zugriff auf die Website der MB zu belegen. Auch sei es rechtlich erforderlich, einen risikobasierten Ansatz zu berücksichtigen.

I.25. Zur Vorbereitung der Beschwerdeverhandlung übermittelten die bB (OZ 23 zu W245 2252208-1), der BF1 (OZ 24 zu W245 2252208-1) und BF2 (OZ 25 zu W245 2252208-1) Stellungnahmen. In diesen Stellungnahmen bekräftigten die Parteien ihre bisher im Verfahren vertretenen Standpunkte.

I.26. Das BVwG führte in der gegenständlichen Rechtssache am 31.03.2023 eine öffentliche mündliche Verhandlung durch, an der der BF1 im Beisein seines bevollmächtigten Vertreters persönlich teilnahm. Ebenso nahm ein Vertreter der bB und der BF2 an der Verhandlung teil. Nach Schluss der mündlichen Verhandlung erfolgte eine mündliche Verkündung des Erkenntnisses. Der BF1 und die BF2 beantragten fristgerecht beim BVwG die schriftliche Ausfertigung des mündlich verkündeten Erkenntnisses.

II. Das Bundesverwaltungsgericht hat erwogen:

II.1. Feststellungen:

Der entscheidungsrelevante Sachverhalt steht fest.

II.1.1. Zum Verfahrensgang:

Der unter Punkt I dargestellte Verfahrensgang wird festgestellt und der Entscheidung zu Grunde gelegt.

II.1.2. Zum Inhaber der Website XXXX :

Die XXXX hat die Website XXXX im Rahmen eines Asset Deals mit der Wirkung zum 01.02.2021 auf die XXXX , München übertragen. Im Anschluss wurde die XXXX in XXXX umbenannt.

Bis August 2021 betreute die XXXX weiterhin im Auftrag und unter Weisung der XXXX , München die Website XXXX .

Im August 2021 erfolgte die komplette Übertragung der Website XXXX in die IT Umgebung der XXXX München. Nach der Übertragung wird XXXX -Analytics mit einem vorgeschalteten Proxy-Server eingesetzt. Dadurch wird eine Übermittlung der IP-Adressen an die BF2 sogar gänzlich unterbunden.

II.1.3. Zur verfahrensgegenständlichen Datenverarbeitung:

Der BF1 besuchte zumindest am 14. August 2020, um 10:45 Uhr, die Website der MB XXXX .

In der Transaktion zwischen dem Browser des BF1 und https://tracking. XXXX wurden am 14. August 2020 um 12:46:19.344 MEZ einzigartige Nutzer-Identifikations-Nummern zumindest in den Cookies „_ga“ und „_gid“ gesetzt. In Folge wurden diese Kennnummern am 14. August 2020 um 12:46:19.948 MEZ an https://www. XXXX -analytics.com/ und somit an die BF2 übermittelt.

Konkret wurden folgende Nutzer-Identifikations-Nummern, die sich im Browser des BF1 befinden, an die BF2 übermittelt (gleiche Werte, die jeweils in verschiedenen Transaktionen aufgetreten sind, wurden jeweils kursiv dargestellt bzw. orange und grün gekennzeichnet):

Domain	Name	Wert	Zweck

https://tracking. XXXX	_ga	*GA1.2.1284433117.1597223478*	XXXX Analytics
https://tracking. XXXX	_gid	*GA1.2.929316258.1597394734*	XXXX Analytics
https://tracking. XXXX	_gads	ID=d77676ed5b074d05:T=1597223569: S=ALNI_MZcJ9EjC13lsaY1Sn8Qu5ovyKMhPw	XXXX Werbung
https://www. XXXX -analytics.com/	_gid	*929316258.1597394734*	XXXX Analytics
https://www. XXXX -analytics.com/	cid	*1284433117.1597223478*	XXXX Analytics

Diese Kennnummern enthalten jeweils eine vorangestellte Zufallszahl und am Ende einen UNIX-Zeitstempel, aus dem sich ergibt, wann das jeweilige Cookie gesetzt wurde. Die Kennnummer im _gid-Cookie mit dem UNIX-Zeitstempel „1597394734“ wurde am Mittwoch, 14. August 2020, um 11:11 und 18 Sekunden MEZ gesetzt, jene im cid-Cookie mit dem UNIX-Zeitstempel „1597223478“ am Freitag, 12 August 2020, um 10:45 und 34 Sekunden MEZ.

Mithilfe dieser Kennnummern ist es für die BF2 möglich, Website-Besucher zu unterscheiden und auch die Information zu erhalten, ob es sich um einen neuen oder um einen wiederkehrenden Website-Besucher von www. XXXX handelt. Jedoch ist eine Website-übergreifende Analyse des Verhaltens auf Basis dieser Kennzahl nicht möglich.

Darüber hinaus wurden jedenfalls auch folgende Informationen (Parameter) über den Browser des BF1 im Zuge von Anfragen (Requests) an https://www. XXXX -analytics.com/collect an den BF2 übermittelt (Auszug aus der HAR-Datei, Request URL https://www. XXXX -analytics.com/collect, Auszug der Anfrage mit Zeitstempel 2020-08-14T10:46:19.924+02:00):

General

- Request URL https://www. XXXX -analytics.com/collect
- Request Method GET
- HTTP Version HTTP/2

– Remote Address XXXX

Headers

- Accept: image/webp,*/*
- Accept-Encoding: gzip, deflate, br
- Accept-Language: en-US,de;q=0.7,en;q=0.3
- Connection: keep-alive

- Host: www. XXXX -analytics.com
- Referer: https://www. XXXX .at/
- TE: Trailers
- User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:79.0) Gecko/20100101 Firefox/79.0

Query Arguments

- _gid: 929316258.1597394734
- _s: 1
- _u: QACAAEAB~
- _v: j83
- a: 443943525
- cid: 1284433117.1597223478
- de: UTF-8
- dl: https://www. XXXX .at/
- dt: XXXX .at Startseite - XXXX
- ea: /
- ec: Scrolltiefe
- el: 25
- gjid:
- gtm: 2wg871PHBM94Q
- je: 0
- jid:
- ni: 0
- sd: 24-bit
- sr: 1280x1024
- t: event
- tid: UA-259349-1
- ul: en-us
- v: 1
- vp: 1263x882
- z: 1764878454

Size

- 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 XXXX handelt es sich um jene der BF2.

Die IP-Adresse des Geräts des BF1 wird im Rahmen dieser Anfragen an https://www. XXXX -analytics.com/collect an die BF2 übermittelt. Verfahrensgegenständlich wurde die IP-Adresse des BF1 an die BF2 übermittelt.

Der BF1 hat am 14.08.2020 im Homeoffice gearbeitet. Im Homeoffice nützt der BF2 einen Bildschirm mit einer Auflösung von 1280x1024 (sr-Wert). Zudem wurde dem sichtbaren Teil des Webfensters eine Größe von 1263x882 (vp-Wert) übermittelt.

II.1.3.1. Zur zusammenfassenden Darstellung der Informationen, welche am 14.08.2020 der BF2 übermittelt wurden:

Als Folge der Implementierung des Tools XXXX -Analytics wurden am 14.08.2020 – zusammengefasst – folgende Informationen vom Browser des BF1, der die Website XXXX besucht hat, an die Server der BF2 übermittelt:

- einzigartige Online-Kennungen (unique identifier), die sowohl den Browser bzw. das Gerät des BF1 als auch die MB (durch die XXXX -Analytics-Account-ID der MB als Websitebetreiberin) identifizieren;
- die Adresse und den HTML-Titel der Website sowie die Unterseiten, die der BF1 besucht hat;
- Informationen zum Browser, Betriebssystem, Bildschirmauflösung, Sprachauswahl sowie Datum und Uhrzeit des Website-Besuchs;
- die IP-Adresse des Geräts, welches der BF1 verwendet hat.

II.1.3.2. Zu Informationen zu den verwendeten Cookies:

Für Universal Analytics kann die JavaScript-Bibliothek analytics.js oder die JavaScript-Bibliothek gtag.js verwendet werden. In beiden Fällen verwenden die Bibliotheken first-party-Cookies, um:

- Eindeutige Benutzer zu unterscheiden und

- die Anfragerate zu drosseln

Bei Verwendung des empfohlenen JavaScript-Snippets werden Cookies auf der höchstmöglichen Domain-Ebene gesetzt. Wenn ihre Website-Adresse zum Beispiel blog.example.co.uk lautet, setzen analytics.js und gtag.js die Cookie-Domain auf.example.co.uk. Das Setzen von Cookies auf der höchstmöglichen Domain-Ebene ermöglicht die Messung über Subdomains hinweg, ohne dass eine zusätzliche Konfiguration erforderlich ist.

Hinweis: gtag.js und analytics.js erfordern kein Setzen von Cookies, um Daten an XXXX -Analytics zu übertragen.

gtag.js und analytics.js setzen die folgenden Cookies:

Cookie-Name	Standard-Ablaufzeit	Beschreibung
_ga	2 Jahre	Wird zur Unterscheidung von Benutzern verwendet.
_gid	24 Stunden	Wird zur Unterscheidung von Nutzern verwendet.
_gat	1 Minute	Wird verwendet, um die Anfragerate zu drosseln. Wenn XXXX Analytics über den XXXX Tag Manager eingesetzt wird, wird dieses Cookie _dc_gtm_<property- id> genannt.
AMP_TOKEN	30 Sekunden bis 1 Jahr	Enthält ein Token, das zum Abrufen einer Client-ID vom AMP-Client-ID-Dienst verwendet werden kann. Andere mögliche Werte zeigen Optout, Inflight-Anfrage oder einen Fehler beim Abrufen einer Client-ID vom AMP-Client-ID-Dienst an.
gac<property-id>	90 Tage	Enthält kampagnenbezogene Informationen für den Benutzer. Wenn Sie Ihre XXXX Analytics- und XXXX Ads-Konten verknüpft haben, lesen die Website-Conversion-Tags von XXXX Ads dieses Cookie, sofern Sie sich nichtabmelden.

II.1.3.3. Zur Verknüpfung mit dem XXXX -Konto des BF1:

Während des Besuchs auf der Website XXXX war der BF1 in seinem XXXX -Konto eingeloggt, welches mit der E-Mail-Adresse XXXX verknüpft ist. Diese E-Mail-Adresse gehört dem BF1.

Bei einem XXXX -Konto handelt es sich um ein Benutzerkonto, welches zur Authentifizierung bei verschiedenen XXXX -Onlinediensten der BF2 dient. So ist ein XXXX -Konto etwa Voraussetzung für die Nutzung von Diensten wie „ XXXX “ oder „ XXXX Drive“ (ein Filehosting-Dienst).

Am 14.08.2020 war im XXXX -Konto des BF1 (XXXX) die Web-&-App Aktivitäten Einstellung aktiviert. Allerdings hat das XXXX -Konto des BF1 sich dagegen entschieden, Aktivitäten von Websites einzuschließen, die XXXX -Dienste nutzen.

Entgegen den eigenen Ausführungen der BF2 ist sie technisch in der Lage, die Information zu bekommen, dass ein bestimmter XXXX -Account-Nutzer die Website XXXX (auf der XXXX -Analytics implementiert ist) besucht hat, sofern dieser XXXX -Account-Nutzer während des Besuchs der Website XXXX im XXXX -Account eingeloggt war.

Metadaten von XXXX -Anwendungen (wie von XXXX -Account), die der BF1 am 14.08.2020 genutzt hat, wurden auf Servern in den Vereinigten Staaten gespeichert.

II.1.3.4. Zur (nicht)anonymisierten Verarbeitung der IP-Adresse des BF1:

Auf der Website der MB XXXX wurde fehlerhaft die IP-Anonymisierungsfunktion implementiert. Dadurch wurde nicht sichergestellt, dass am 14.08.2020 nach Übermittlung von Daten an die BF2 die IP-Adresse anonymisiert wurde.

II.1.3.5. Zu den gelöschten Informationen:

Die MB hat die BF2 im Laufe des verwaltungsbehördlichen Verfahrens angewiesen, alle über die XXXX -Analytics Properties gesammelten Daten für die Website XXXX zu löschen. Die BF2 hat die Löschung durchgeführt.

II.1.3.6. Zur Deklaration von personenbezogenen Daten durch die BF2:

Auf der Seite „Datenverarbeitungsbedingungen für XXXX Werbeprodukte: Informationen zu den Diensten“ gibt die BF2 an, dass im Rahmen des Auftragsverarbeitungsdienstes „ XXXX Analytics“ die Daten „Online-Kennzeichnungen (einschließlich Cookie-Kennungen), Internet-Protokoll-Adressen und Gerätekennungen und vom Kunden vergebene Kennzeichnungen“ personenbezogene Daten sein können.

II.1.4. Zum Webanalysedienst XXXX -Analytics:

XXXX -Analytics ist ein Messdienst, der es Kunden ermöglicht, Traffic zu Eigenschaften zu messen, einschließlich des Traffic von Besuchern, die die Website eines Website-Besitzers besuchen. Webanalysedienste sind eine beliebte Kategorie von Diensten, die von mehreren Anbietern angeboten werden und gelten als ein wesentliches Werkzeug für den Betrieb einer Website.

Website-Besitzer sind auf Webanalysedienste wie XXXX -Analytics angewiesen, um ihnen zu helfen, zu verstehen, wie Website-Besucher mit ihrer Website und ihren Diensten interagieren. XXXX -Analytics hilft ihnen dabei, ansprechendere Inhalte zu erstellen und die Stabilität ihrer Websites zu überwachen und zu erhalten.

Zudem können Website-Besitzer Dashboards einrichten, die einen Überblick über Berichte und Metriken geben, die Kunden am meisten interessieren, zB. in Echtzeit die Anzahl der Besucher auf einer Website überwachen. XXXX -Analytics kann auch helfen, die Wirksamkeit

von Werbekampagnen, die Website-Besitzer auf XXXX -Anzeigendiensten durchführen, zu messen und zu optimieren.

Alle durch XXXX -Analytics erhobenen Daten werden in den Vereinigten Staaten gehostet (gespeichert und weiterverarbeitet).

II.1.5. Zur Implementierung und Funktionsweise von XXXX -Analytics:

Der Webanalysedienst XXXX -Analytics wird durch die Einbindung eines Blocks eines JavaScript-Codes auf der Seite des Website-Besitzers eingebettet. Wenn Benutzer einer Webseite eine Seite ansehen, verweist dieser JavaScript-Code auf eine zuvor auf das Gerät des Benutzers heruntergeladene JavaScript-Datei, die dann den Tracking-Betrieb für XXXX -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 sind.

Die Daten, die XXXX -Analytics im Auftrag des Website-Besitzers erhebt, stammen aus diesen Quellen:

- Die HTTP-Anfrage des Benutzers
- Browser/Systeminformationen
- First-Party-Cookies

Eine HTTP-Anfrage für jede Webseite enthält Details über den Browser und den Computer, der die Anfrage stellt, wie zB. Hostname, Browsertyp, Referrer und Sprache. Darüber hinaus bietet das Document Objekt Model (DOM) der meisten Browser Zugriff auf detailliertere Browser- und Systeminformationen, wie Java- und Flash-Unterstützung und Bildschirmauflösung. XXXX -Analytics nutzt diese Informationen. XXXX -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, wird es an die Analytics-Server in Form einer langen Liste von Parametern gesendet, die an eine einzelne GIF-Bildanfrage an die Domain XXXX -analytics.com gesendet werden. Die in der GIF-Anfrage enthaltenen Daten sind die Daten, die an die XXXX -Analytics-Server gesendet werden, die dann weiterverarbeitet werden und in den Berichten des Website-Besitzers enden.

II.1.6. Zur Einbettung des Programmcodes für XXXX -Analytics auf der Website XXXX der Mitbeteiligten:

Aufgrund einer Entscheidung der MB wurde der Programmcode für XXXX -Analytics auf ihrer Website eingebettet.

Durch die Konfiguration der Tags bzw. Aktivierung bzw. Deaktivierung verschiedener XXXX -Analytics-Funktionen über die Benutzeroberfläche bestimmte die MB die Nutzung der erhobenen Daten. Beispielsweise konnte die MB die Dauer der Aufbewahrungsfrist für Daten festlegen, anweisen, dass die IP-Adresse nach Eingang bei der BF2 anonymisiert wird, festlegen wer Daten empfangen darf, usw.

II.1.7. Zur Rechtsgrundlage für die Nutzung von XXXX -Analytics durch die Mitbeteiligte:

Die Nutzung von XXXX -Analytics setzt einen Vertrag voraus.

Die MB und BF2 haben einen Vertrag mit dem Titel „Auftragsdatenverarbeitungsbedingungen für XXXX Werbeprodukte“ abgeschlossen. Dieser Vertrag hatte in der Version vom 12.08.2020 (VWA ./18) zumindest am 14. August 2020 Gültigkeit. Der Vertrag regelt Auftragsdatenverarbeitungsbedingungen für XXXX Werbeprodukte. Er gilt für die Bereitstellung von Auftragsverarbeiterdiensten und damit im Zusammenhang stehende technischen Supportleistungen für Kunden (MB) der BF2. Die MB nutzte die kostenlose Version von XXXX -Analytics.

Der Webanalysedienst XXXX -Analytics fällt unter den Anwendungsbereich der „Auftragsdatenverarbeitungsbedingungen für XXXX Werbeprodukte“.

In Bezug auf die Auftragsdatenverarbeitungsbedingungen für XXXX Werbeprodukte können im Zusammenhang mit dem Webanalysedienst XXXX -Analytics Online-Kennzeichnungen (einschließlich Cookie-Kennungen), Internet-Protokoll-Adressen und Gerätekennungen sowie vom Kunden vergebene Kennzeichnungen personenbezogene Daten des Kunden (MB) darstellen.

Zudem sehen diese Auftragsdatenverarbeitungsbedingungen in Punkt 10.2. die Anwendung von Standarddatenschutzklauseln vor, wenn eine Übermittlung von personenbezogenen Daten des Kunden aus dem EWR in ein Drittland erfolgt, das nicht einer Angemessenheitsentscheidung nach den europäischen Datenschutzvorschriften unterliegt. Darauf aufbauend haben die MB und die BF2 am 12.08.2020 einen zweiten Vertrag mit dem Titel „ XXXX Ads Data Processing Terms: Model Contract Clauses, Standard Contractual Clauses for Processors“ (VWA ./22) abgeschlossen. Dabei handelt es sich um Standardvertragsklauseln für den internationalen Datenverkehr (auf Grundlage eines 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.).

Zusätzlich zur Implementierung von XXXX -Analytics kann ein Website-Besitzer seine Analysedaten an XXXX weitergeben, indem er die Datenfreigabe-Einstellung von XXXX

Produkten und Dienstleistungen aktiviert und die Datenschutzbestimmungen für XXXX Measurement Controller-Controller, die für die Verwendung dieser Einstellung gelten, gesondert akzeptiert.

Die Datenfreigabe-Einstellung ist von der MB nicht aktiviert worden. Auch setzte die MB XXXX -Signals nicht ein. Die MB verfügte über kein eigenes Authentifizierungssystem und benutze auch keine Benutzer-ID-Funktion.

II.1.8. Zum Zweck der Verarbeitung durch die Mitbeteiligte:

XXXX -Analytics wird eingesetzt, um folgende allgemeine statistische Auswertungen über das Verhalten der Websitebesucher zu ermöglichen:

- Reichweitenmessung (also wie viele User rufen die Seite auf);
- Auswertung, welche Artikel den größten Traffic haben (also welche Artikel am meisten aufgerufen wurden),
- Durchschnittliche Sitzungsdauer,
- Auswertung der durchschnittlichen Anzahl an Seiten, die pro Sitzung aufgerufen werden.

II.1.9. Zu den Maßnahmen der BF2 nach dem Urteil des Europäischen Gerichtshofes vom 16.07.2020 in der Rechtssache C-311/18:

Die BF2 ging nach der Entscheidung des Europäischen Gerichtshofes davon aus, dass das Urteil auch für die Nutzung von XXXX -Analytics durch Website-Besitzer gilt. Nach der Entscheidung des Europäischen Gerichtshofes begann die BF2 sofort mit der Änderung der Auftragsdatenverarbeitungsbedingungen (DTPS), um die Standardvertragsklauseln (SCC) für alle betroffenen Verträge anwendbar zu machen. Dazu gehörten die Aktualisierung einer Vielzahl von Verträgen, die Übermittlung von Mitteilungen an Website-Besitzer am 03.08.2020, die Übersetzungen und die Veröffentlichung der entsprechenden Vertragsbedingungen. Diese Änderungen der Auftragsdatenverarbeitungsbedingungen (DTPS) traten am 12.08.2020 in Kraft.

Die aktualisierten Auftragsdatenverarbeitungsbedingungen (DTPS) sehen in Abschnitt 10 vor, dass, soweit die Speicherung und/oder Verarbeitung personenbezogener Daten von Kunden, einschließlich personenbezogener Daten in XXXX -Analytics-Daten, die Übermittlung personenbezogener Daten von Kunden aus dem EWR in ein Drittland umfasst, das nicht einer Angemessenheitsentscheidung gemäß der DSGVO unterliegt, der Website-Besitzer (als Datenexporteur) bei XXXX (als Datenimporteur) für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern, die keinen angemessenen Datenschutz

gewährleisten, Standardvertragsklauseln (SCCs) verwendet. Die Standardvertragsklauseln (SCCs) werden unter XXXX zur Verfügung gestellt. Diese Standardvertragsklauseln (SCCs) würden den von der Europäischen Kommission in ihrem Beschluss 2010/87/EU veröffentlichten Klauseln entsprechen.

II.1.10. Zu den ergänzenden Maßnahmen, die mit Einführung der Standardvertragsklauseln von der BF2 gesetzt wurden:

Folgende Maßnahmen waren vor der Entscheidung des Europäischen Gerichtshofes in der Rechtssache C-311/18 in Kraft und bestanden daher auch während der Zeit, in der die Bedingungen bis zum 12.08.2020 aktualisiert wurden. Nach den Ausführungen der BF2 seien diese Maßnahmen geeignet, um ein angemessenes Schutzniveau zu gewährleisten.

II.1.10.1. Rechtliche und organisatorische Maßnahmen:

Die BF2 wertet jede Anfrage aus, die diese von den staatlichen Behörden auf Nutzerdaten erhält, um sicherzustellen, dass sie die geltenden Gesetze und die XXXX -Richtlinien erfüllen.

Die BF2 benachrichtigt Kunden, bevor eine ihrer Informationen bekannt gegeben wird, es sei denn, eine solche Mitteilung ist gesetzlich verboten oder die Anfrage beinhaltet einen Notfall.

Die BF2 veröffentlicht einen Transparenzbericht.

Die BF2 veröffentlicht ihre Politik im Umgang mit Regierungsanfragen.

II.1.10.2. Technische Maßnahmen:

Die BF2 setzt robuste technische Maßnahmen ein, um personenbezogene Daten während der Übertragung zu schützen (standardmäßige Verwendung von http Strict Transport Security (HSTS), Verschlüsselung von Daten auf einer oder mehreren Netzwerkschichten (Schutz der Kommunikation zwischen XXXX -Diensten, Schutz von Daten im Transit zwischen Rechenzentren und Schutz der Kommunikation zwischen Nutzern und Websites)).

Die BF2 setzt robuste technische Maßnahmen ein, um gespeicherte personenbezogene Daten zu schützen (Die BF2 verschlüsselt XXXX -Analytics-Daten, die in ihren Rechenzentren gespeichert werden; die BF2 baut Server ausschließlich für ihre Rechenzentren und unterhält ein branchenführendes Sicherheitsteam, ein Zugriff auf XXXX -Analytics-Daten erfolgt nur für Mitarbeiter, die die Daten für ihre Arbeit benötigen).

II.1.10.3. Pseudonymität der Daten von XXXX -Analytics:

Ist die BF2 der Ansicht, dass die Daten zur Messung durch Website-Besitzer personenbezogene Daten sind, müssten diese als pseudonym betrachtet werden. Die BF2 ist der Ansicht, dass bei einem Zugriff eines Dritten auf die XXXX -Analytics Daten, dieser

grundsätzlich nicht in der Lage sein wird, die betroffene Person anhand dieser Daten zu identifizieren.

II.1.10.4. Optionale technische Maßnahme – IP-Anonymisierung:

Zusätzlich zu den genannten Maßnahmen können Website-Besitzer die „IP-Anonymisierung" nutzen, um die BF2 anzuweisen, alle IP-Adressen unmittelbar nach ihrer Erhebung zu anonymisieren und so zur Datenminimierung beizutragen. Sofern dies verwendet wird, wird zu keinem Zeitpunkt die vollständige IP-Adresse auf eine Festplatte geschrieben, da alle Anonymisierung im Speicher fast augenblicklich erfolgt, nachdem die Anfrage bei der BF2 eingegangen ist.

II.1.11. Die BF2 als elektronischer Kommunikationsdienst:

Die BF2 ist als Anbieter elektronischer Kommunikationsdienste im Sinne von 50 U.S.Code § 1881(b)(4) zu qualifizieren und unterliegt als solcher der Überwachung durch US-Geheimdienste gemäß 50 U.S.Code § 1881a („FISA 702"). Die BF2 übermittelt der US-Regierung gemäß U.S.Code § 1881a personenbezogene Daten. Es können von der US-Regierung Metadaten und Inhaltsdaten angefordert werden.

II.2. Beweiswürdigung:

Beweis wurde erhoben durch Einsicht in den Verwaltungsakt der bB [in der Folge kurz „VWA" mit den Bestandteilen ./01 – Datenschutzbeschwerde des BF1 vom 18.08.2020 (siehe Punkt I.1), ./02 – Datenschutzbeschwerde des BF1 vom 18.08.2020 – Beilage – Nutzungsbedingungen für XXXX Analytics (siehe Punkt I.1), ./03 – Datenschutzbeschwerde des BF1 vom 18.08.2020 – Beilage – Nutzungsbedingungen für Auftragsdatenverarbeitungsbedingungen für XXXX Werbeprodukte, Version 01.01.2020 (siehe Punkt I.1), ./04 – Datenschutzbeschwerde des BF1 vom 18.08.2020 – Beilage – Nutzungsbedingungen für Auftragsdatenverarbeitungsbedingungen für XXXX Werbeprodukte, Version 12.08.2020 (siehe Punkt I.1), ./05 – Datenschutzbeschwerde des BF1 vom 18.08.2020 – Beilage – HAR-Daten des Website-Besuchs (siehe Punkt I.1), ./06 – Datenschutzbeschwerde des BF1 vom 18.08.2020 – Beilage – XXXX (siehe Punkt I.1), ./07 – Datenschutzbeschwerde des BF1 vom 18.08.2020 – Beilage – Vertretungsurkunde (siehe Punkt I.1), ./08 – Ermittlung der federführenden Zuständigkeit (siehe Punkt I.2), ./09 – Bescheid der bB betreffend Aussetzung des Verfahrens (siehe Punkt I.2), ./10 – Aufforderung der bB zur Stellungnahme an die MB (siehe Punkt I.2), ./11 – Stellungnahme der MB vom 16.12.2020 (siehe Punkt I.3), ./12 – Stellungnahme der MB vom 16.12.2020 – Beilage – Berichte aus dem Tool (siehe Punkt I.3), ./13 – Stellungnahme der MB vom 16.12.2020 – Beilage – Informationen zur IP-Anonymisierung (siehe Punkt I.3), ./14 – Stellungnahme der MB vom 16.12.2020 – Beilage – Screenshot zur eingestellten Speicherdauer (siehe Punkt I.3),

./15 – Stellungnahme der MB vom 16.12.2020 – Beilage – Liste der Serverstandorte (siehe Punkt I.3), ./16 – Stellungnahme der MB vom 16.12.2020 – Beilage – Auftragsdatenverarbeitungsbedingungen für XXXX Werbeprodukte, Version 16.08.2020 (siehe Punkt I.3), ./17 – Stellungnahme der MB vom 16.12.2020 – Beilage – Auftragsdatenverarbeitungsbedingungen für XXXX Werbeprodukte, Version 12.08.2020 (siehe Punkt I.3), ./18 – Stellungnahme der MB vom 16.12.2020 – Beilage – Auftragsdatenverarbeitungsbedingungen für XXXX Werbeprodukte, Version 01.01.2020 (siehe Punkt I.3), ./19 – Stellungnahme der MB vom 16.12.2020 – Beilage – Vergleichsversion AVV vom 01.01.2020 vs 12.08.2020 (siehe Punkt I.3), ./20 – Stellungnahme der MB vom 16.12.2020 – Beilage – Vergleichsversion AVV vom 12.08.2020 vs 16.08.2020(siehe Punkt I.3), ./21 – Stellungnahme der MB vom 16.12.2020 – Beilage – Screenshot zu Einstellungen (siehe Punkt I.3), ./22 – Stellungnahme der MB vom 16.12.2020 – Beilage – Standarddatenschutzklauseln (siehe Punkt I.3), ./23 – Stellungnahme der MB vom 16.12.2020 – Beilage – Informationen zu Sicherheitsmaßnahmen (siehe Punkt I.3), ./24 – Stellungnahme der MB vom 16.12.2020 – Beilage – Verzeichnis von Verarbeitungstätigkeiten zu XXXX Analytics (siehe Punkt I.3), ./25 – Aufforderung der bB zur Stellungnahme an BF1 vom 21.12.2020 (siehe Punkt I.4), ./26 – Stellungnahme des BF1 vom 22.01.2021 (siehe Punkt I.4), ./27 – Stellungnahme des BF1 vom 22.01.2021 – Beilage – Drittpartner im Cookiebanner der MB (siehe Punkt I.4), ./28 – Stellungnahme des BF1 vom 22.01.2021 – Beilage – Kontakte von XXXX mit US-Server (siehe Punkt I.4), ./29 – Stellungnahme des BF1 vom 22.01.2021 – Beilage – Kontakte von XXXX mit US-Server, Hinweis auf Fingerprinttechnologie (siehe Punkt I.4), ./30 – Aufforderung der bB zur Stellungnahme an BF2 vom 26.02.2021 (siehe Punkt I.5), ./31 – Stellungnahme der BF2 vom 09.04.2021 (siehe Punkt I.5), ./32 – Aufforderung der bB zur Stellungnahme an BF1 und MB vom 14.04.2021 (siehe Punkt I.6), ./33 – Stellungnahme des MB vom 04.05.2021 (siehe Punkt I.7), ./34 – Stellungnahme des BF1 vom 05.05.2021 (siehe Punkt I.8), ./35 – Stellungnahme des BF1 vom 05.05.2021 – Beilage – XXXX -Analytics Cookie, Verwendung auf Website (siehe Punkt I.8), ./36 – Stellungnahme des BF1 vom 05.05.2021 – Beilage – So verwendet XXXX Cookies (siehe Punkt I.8), ./37 – Stellungnahme des BF1 vom 05.05.2021 – Beilage – Measurement Protocol Parameter Reference (siehe Punkt I.8), ./38 – Aufforderung der bB zur Stellungnahme an BF1 vom 06.05.2021 (siehe Punkt I.9), ./39 – Aufforderung der bB zur Stellungnahme an BF2 vom 06.05.2021 (siehe Punkt I.9), ./40 – Aufforderung der bB zur Stellungnahme an MB vom 10.05.2021 (siehe Punkt I.9), ./41 – Antrag der BF2 auf Verlängerung der Frist zur Stellungnahme vom 12.05.2021 (siehe Punkt I.9), ./42 – Gewährung der beantragten Fristerstreckung durch die BB vom 14.05.2021 (siehe Punkt I.9), ./43 – Stellungnahme der BF2 vom 14.05.2021 (siehe Punkt I.10), ./44 – Aufforderung der bB zur Stellungnahme an BF1 und MB vom 11.06.2021 (siehe Punkt I.11), ./45 – Antrag des BF1

auf Verlängerung der Frist zur Stellungnahme vom 11.06.2021 (siehe Punkt I.11), ./46 – Aufforderung der bB zur Stellungnahme an MB vom 16.06.2021 (siehe Punkt I.11), ./47 – Stellungnahme der MB (Übertragung) vom 18.06.2021 (siehe Punkt I.12), ./48 – Stellungnahme der MB (Konfigurationsfehler, Löschung von Daten) vom 18.06.2021 (siehe Punkt I.13), ./49 – Stellungnahme der MB (Konfigurationsfehler, Löschung von Daten) vom 18.06.2021 – Beilage – Mitteilung der BF2 über die Löschung von Informationen (siehe Punkt I.13), ./50 – Stellungnahme der MB (Konfigurationsfehler, Löschung von Daten) vom 18.06.2021 – Beilage – Darstellung über die falsche und richtige Implementierung der Anonymisierungsfunktion (siehe Punkt I.13), ./51 – Übermittlung der Stellungnahme der MB (VWA ./48 bis ./50) an BF1 (siehe Punkt I.13), ./52 – Mitteilung der MB vom 24.06.2021 (siehe Punkt I.13), ./53 – Mitteilung der MB vom 24.06.2021 – Beilage – Löschungsbestätigung der BF2 (siehe Punkt I.13), ./54 – Stellungnahme der BF2 vom 09.07.2021 (siehe Punkt I.14), ./55 – Stellungnahme des BF1 vom 09.07.2021 (siehe Punkt I.15), ./56 – Aufforderung der bB zur Stellungnahme an BF1 vom 22.07.2021 (siehe Punkt I.16), ./57 – Stellungnahme der BF2 vom 12.08.2021 (siehe Punkt I.16), ./58 – Website Evidence Collection betreffend Website der MB, ./59 – Teilbescheid der bB vom 22.12.2021, zugestellt am 12. und 13.01.2022 (siehe Punkt I.17), ./60 – Bescheidbeschwerde des BF1 vom 07.02.2022 (siehe Punkt I.20), ./61 – Stellungnahme der bB zur Bescheidbeschwerde des BF1 vom 15.02.2022, ./62 – Bescheidbeschwerde der BF2 vom 09.02.2022 (siehe Punkt I.18), ./63 – Bescheidbeschwerde der BF2 vom 09.02.2022 – Beilage – Cookies und User Identification (siehe Punkt I.18), ./64 – Bescheidbeschwerde der BF2 vom 09.02.2022 – Beilage – Linker (siehe Punkt I.18), ./65 – Bescheidbeschwerde der BF2 vom 09.02.2022 – Beilage – Report XXXX (siehe Punkt I.18), ./66 – Bescheidbeschwerde der BF2 vom 09.02.2022 – Beilage – New EU-US data transfer Framework (siehe Punkt I.18), ./67 – Stellungnahme der bB zur Bescheidbeschwerde der BF2 vom 17.02.2022 (siehe Punkt I.19), ./68 – Stellungnahme der bB zur Bescheidbeschwerde der BF2 vom 17.02.2022 – Beilage – Entscheidung des Europäischen Datenschutzbeauftragten vom 05.01.2022 (siehe Punkt I.19), ./69 – Stellungnahme der bB zur Bescheidbeschwerde der BF2 vom 17.02.2022 – Beilage – Entscheidung des LG München vom 20.02.2022 (siehe Punkt I.19), ./70 – Stellungnahme der bB zur Bescheidbeschwerde der BF2 vom 17.02.2022 – Beilage – Gutachten zum aktuellen Stand des US-Überwachungsrechts (siehe Punkt I.19) und ./71 – Stellungnahme der bB zur Bescheidbeschwerde der BF2 vom 17.02.2022 – Beilage – Wesentliche Befunde des Gutachtens zum aktuellen Stand des US-Überwachungsrechts (siehe Punkt I.19)] sowie in den Gerichtsakt des BVwG (Aktenbestandteile werden mit Ordnungszahl, kurz „OZ“ gekennzeichnet).

II.2.1. Zum Verfahrensgang:

Der oben angeführte Verfahrensgang ergibt sich aus dem unbedenklichen und unzweifelhaften Akteninhalt des vorgelegten Verwaltungsaktes der bB und des Gerichtsaktes des BVwG.

II.2.2. Zum Inhaber der Website XXXX

Die dahingehenden Feststellungen ergeben sich zweifelsfrei aus der Stellungnahme der MB vom 18.06.2021 (VWA ./47).

II.2.3. Zur verfahrensgegenständlichen Datenverarbeitung:

Die dahingehenden Feststellungen ergeben sich zweifelsfrei aus den Feststellungen des bekämpften Bescheides (VWA ./59, Seite 18 ff), der Stellungnahme des BF1 vom 05.05.2021 (VWA ./34) und der Bescheidbeschwerde der BF2 (VWA ./62, Seite 6).

Die Feststellung, dass verfahrensgegenständlich die IP-Adresse des BF1 an die BF2 übermittelt wurde, ergibt sich aus den Ausführungen des BF1 bzw. seines Vertreters in der Beschwerdeverhandlung. In diesem Zusammenhang war die vom Vertreter des BF1 dargestellte VPN-Lösung nachvollziehbar und wurde in der Folge von der BF2 in der Beschwerdeverhandlung nicht mehr in Frage gestellt. Zudem hat der BF1 am 14.08.2020 glaubhaft im Homeoffice gearbeitet. Dies ergibt sich aus den glaubhaften Ausführungen des BF1, dass er im Jahr 2020 corona-bedingt überwiegend im Homeoffice gearbeitet habe und aufgrund der Nutzung eines hohen/schmalen Monitors (Verhandlungsprotokoll vom 31.03.2022, OZ 29 zu W245 2252208, Seite 14). Sohin waren dahingehende Feststellungen zu treffen.

II.2.3.1. Zur zusammenfassenden Darstellung der Informationen, welche am 14.08.2020 der BF2 übermittelt wurden:

Die dahingehenden Feststellungen ergeben sich zweifelsfrei aus den Ausführungen der bB im bekämpften Bescheid (VWA ./59, Seite 27).

II.2.3.2. Zu Informationen zu den verwendeten Cookies:

Die dahingehenden Feststellungen ergeben sich zweifelsfrei aus Erklärungen des BF1 im verwaltungsbehördlichen Verfahren (VWA ./05) und aus den Feststellungen des bekämpften Bescheides (VWA ./59, Seite 15).

II.2.3.3. Zur Verknüpfung mit dem XXXX -Konto des BF1:

Die dahingehenden Feststellungen ergeben sich zweifelsfrei aus den Feststellungen des bekämpften Bescheides (VWA ./59, Seite 18 ff) und der Stellungnahme der BF2 (VWA ./43, Seite 10 f).

In seiner Stellungnahme vom 09.04.2021 hat der BF2 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 XXXX -Account. Dies widerlegte der BF1 bzw. die bB im Verfahren mit folgender nachvollziehbarer Argumentation: Wenn nämlich dem Wunsch eines XXXX -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 XXXX -Account-Nutzers zu erhalten.

Unabhängig davon standen der BF2 am 14.08.2020 zahlreiche Metadaten zur Verfügung (OZ 25 zu W245 2252208-1, Seite 3), die bei einem Aufruf einer Anwendung (wie z.B. XXXX -Konto) übermittelt werden. Im verfahrensgegenständlichen Zeitpunkt (14.08.2020) hat der BF1 auch sein XXXX -Konto genutzt. Mit den Metadaten, welche bei der Nutzung des XXXX -Kontos übermittelt wurden, war eine Verknüpfung mit den übermittelten Metadaten im Zuge des XXXX (über XXXX -analytics) möglich.

Zudem war zweifelsfrei eine Verknüpfung mit der IP-Adresse möglich. Der BF1 hat am 14.08.2020 im Homeoffice gearbeitet. In diesem Zusammenhang wurde die IP-Adresse direkt vom BF1 der BF2 übermittelt (Verhandlungsprotokoll vom 31.03.2022, OZ 29 zu W245 2252208, Seite 14). Da der BF1 bei seinem Besuch der Website XXXX (XXXX -Analytics) gleichzeitig im XXXX -Konto angemeldet war, kann zwischen diesen Anwendungen problemlos eine Verknüpfung über die IP-Adresse hergestellt werden. Bei beiden Anwendungen wird die IP-Adresse schon aus technischen Gründen übertragen. Vor diesem Hintergrund kann auf Grund der Übertragung der IP-Adresse über die Anwendung XXXX -Analytics, ein Personenbezug zum XXXX -Konto (bzw. zu den Anmeldeinformationen des BF1) hergestellt werden. Da der BF1 zu diesem Zeitpunkt im Homeoffice gearbeitet hat und er alleine lebt, konnte nur er die übermittelte IP-Adresse nutzen.

Aufgrund der einfachen Verknüpfbarkeit von Metadaten und IP-Adresse zwischen den einzelnen Anwendungen (XXXX -Konto und XXXX -Analytics) kann unstrittig ein Personenbezug (Anmeldedaten zum XXXX) hergestellt werden.

Auch war festzustellen, dass Metadaten von XXXX -Anwendungen (wie z.B. XXXX -Account) in die Vereinigten Staaten übertragen wurden, die der BF1 am 14.08.2020 genutzt hat (Verhandlungsprotokoll vom 31.03.2022, OZ 29 zu W245 2252208, Seite 11 f).

II.2.3.4. Zur (nicht)anonymisierten Verarbeitung der IP-Adresse des BF1:

Die dahingehenden Feststellungen ergeben sich zweifelsfrei aus den Erklärungen der MB im verwaltungsbehördlichen Verfahren (VWA ./48)

II.2.3.5. Zu den gelöschten Informationen:

Die dahingehenden Feststellungen ergeben sich zweifelsfrei aus den Erklärungen der MB und der BF2 im verwaltungsbehördlichen Verfahren (VWA ./48, ./49, ./50, ./52 und ./53).

II.2.3.6. Zur Deklaration von personenbezogenen Daten durch die BF2:

Die dahingehenden Feststellungen ergeben sich aus den Ausführungen der bB im Zuge der Aktenvorlage (VWA ./67, Seite 4) sowie aus einer Einsichtnahme in die Seite der BF2 XXXX zuletzt abgerufen am 26.03.2023).

II.2.4. Zum Webanalysedienst XXXX -Analytics:

Die dahingehenden Feststellungen ergeben sich zweifelsfrei aus Erklärungen der BF2 im verwaltungsbehördlichen Verfahren (VWA ./31, Seite 4).

II.2.5. Zur Implementierung und Funktionsweise von XXXX -Analytics:

Die dahingehenden Feststellungen ergeben sich zweifelsfrei aus Erklärungen der BF2 im verwaltungsbehördlichen Verfahren (VWA ./31, Seite 4 f).

II.2.6. Zur Einbettung des Programmcodes für XXXX -Analytics auf der Website XXXX der Mitbeteiligten:

Die dahingehenden Feststellungen ergeben sich zweifelsfrei aus den Unterlagen des vorgelegten Verwaltungsaktes (VWA ./10, Seite 1 und VWA ./31, Seite 7 f)

II.2.7. Zur Rechtsgrundlage für die Nutzung von XXXX -Analytics durch die Mitbeteiligte:

Die dahingehenden Feststellungen ergeben sich zweifelsfrei aus den Unterlagen des vorgelegten Verwaltungsaktes (VWA ./31, Seite 6).

II.2.8. Zum Zweck der Verarbeitung durch die Mitbeteiligte:

Die dahingehenden Feststellungen ergeben sich zweifelsfrei aus den Unterlagen des vorgelegten Verwaltungsaktes (VWA ./10, Seite 2, ./11, Seite 11, ./18, ./21, ./22 Teilbescheid, Seite 15 ff).

II.2.9. Zu den Maßnahmen der BF2 nach dem Urteil des Europäischen Gerichtshofes vom 16.07.2020 in der Rechtssache C-311/18:

Die dahingehenden Feststellungen ergeben sich zweifelsfrei aus Erklärungen der BF2 im verwaltungsbehördlichen Verfahren (VWA ./31, Seite 21 f).

II.2.10. Zu den ergänzenden Maßnahmen, die mit Einführung der Standardvertragsklauseln von der BF2 gesetzt wurden:

Die dahingehenden Feststellungen ergeben sich zweifelsfrei aus Erklärungen der BF2 im verwaltungsbehördlichen Verfahren (VWA ./31, Seite 24 ff und VWA ./43).

II.2.11. Die BF2 als elektronischer Kommunikationsdienst:

Die dahingehenden Feststellungen ergeben sich zweifelsfrei aus dem Gutachten zum aktuellen Stand des US-Überwachungsrechts und der Überwachungsbefugnisse sowie aus dem Transparenzbericht der BF2 XXXX zuletzt abgefragt am 29.03.2023).

II.3. Rechtliche Beurteilung:

II.3.1. Zur Zuständigkeit:

Gemäß § 6 BVwGG entscheidet das Bundesverwaltungsgericht durch Einzelrichter, sofern nicht in Bundes- oder Landesgesetzen die Entscheidung durch Senate vorgesehen ist.

Dem angefochtenen Bescheid liegt eine Entscheidung der bB gemäß Art. 44 DSGVO zugrunde. Diese Angelegenheit ist gemäß § 27 DSG von Senatsentscheidungen erfasst.

Das Verfahren der Verwaltungsgerichte mit Ausnahme des Bundesfinanzgerichtes ist durch das VwGVG, BGBl. I Nr. 33/2013, geregelt (§ 1 leg.cit.). Gemäß § 58 Abs. 2 VwGVG bleiben entgegenstehende Bestimmungen, die zum Zeitpunkt des Inkrafttretens dieses Bundesgesetzes bereits kundgemacht wurden, in Kraft.

Gemäß § 17 VwGVG sind, soweit in diesem Bundesgesetz nicht anderes bestimmt ist, auf das Verfahren über Beschwerden gemäß Art. 130 Abs. 1 B-VG die Bestimmungen des AVG mit Ausnahme der §§ 1 bis 5 sowie des IV Teiles, die Bestimmungen der Bundesabgabenordnung – BAO, BGBl. Nr. 194/1961, des Agrarverfahrensgesetzes – AgrVG, BGBl. Nr. 173/1950, und des Dienstrechtsverfahrensgesetzes 1984 – DVG, BGBl. Nr. 29/1984, und im Übrigen jene verfahrensrechtlichen Bestimmungen in Bundes- oder Landesgesetzen sinngemäß anzuwenden, die die Behörde in dem dem Verfahren vor dem Verwaltungsgericht vorangegangenen Verfahren angewendet hat oder anzuwenden gehabt hätte.

Gemäß § 28 Abs. 1 VwGVG haben die Verwaltungsgerichte die Rechtssache durch Erkenntnis zu erledigen, sofern die Beschwerde nicht zurückzuweisen oder das Verfahren einzustellen ist. Gemäß Abs. 2 leg.cit. hat das Verwaltungsgericht über Beschwerden nach Art. 130 Abs. 1 Z 1 B-VG dann in der Sache selbst zu entscheiden, wenn

1. der maßgebliche Sachverhalt feststeht oder

2. die Feststellung des maßgeblichen Sachverhalts durch das Verwaltungsgericht selbst im Interesse der Raschheit gelegen oder mit einer erheblichen Kostenersparnis verbunden ist.

Wie oben bereits ausgeführt steht der in der Angelegenheit maßgebliche Sachverhalt aufgrund der Aktenlage fest. Das Bundesverwaltungsgericht hat daher in der Sache selbst zu entscheiden.

II.3.2. Zur Rechtslage im gegenständlichen Beschwerdeverfahren:

<u>Art. 4 Z. 1 DSGVO – Begriffsbestimmungen – lautet:</u>

Im Sinne dieser Verordnung bezeichnet der Ausdruck:

1. *" 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, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;*

Art. 44 DSGVO – Allgemeine Grundsätze der Datenübertragung – lautet:

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.

Art. 45 DSGVO – Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses – lautet auszugsweise:

(1) Eine Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation darf vorgenommen werden, wenn die Kommission beschlossen hat, dass das betreffende Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in diesem Drittland oder die betreffende internationale Organisation ein angemessenes Schutzniveau bietet. Eine solche Datenübermittlung bedarf keiner besonderen Genehmigung.

(2) Bei der Prüfung der Angemessenheit des gebotenen Schutzniveaus berücksichtigt die Kommission insbesondere das Folgende:

a) die Rechtsstaatlichkeit, die Achtung der Menschenrechte und Grundfreiheiten, die in dem betreffenden Land bzw. bei der betreffenden internationalen Organisation geltenden einschlägigen Rechtsvorschriften sowohl allgemeiner als auch sektoraler Art – auch in Bezug auf öffentliche Sicherheit, Verteidigung, nationale Sicherheit und Strafrecht sowie Zugang der Behörden zu personenbezogenen Daten – sowie die Anwendung dieser Rechtsvorschriften, Datenschutzvorschriften, Berufsregeln und Sicherheitsvorschriften einschließlich der Vorschriften für die Weiterübermittlung personenbezogener Daten an ein anderes Drittland bzw. eine andere internationale Organisation, die Rechtsprechung sowie wirksame und durchsetzbare Rechte der betroffenen Person und wirksame verwaltungsrechtliche und gerichtliche Rechtsbehelfe für betroffene Personen, deren personenbezogene Daten übermittelt werden,

b) die Existenz und die wirksame Funktionsweise einer oder mehrerer unabhängiger Aufsichtsbehörden in dem betreffenden Drittland oder denen eine internationale Organisation untersteht und die für die Einhaltung und Durchsetzung der Datenschutzvorschriften, einschließlich angemessener Durchsetzungsbefugnisse, für die Unterstützung und Beratung der betroffenen Personen bei der Ausübung ihrer Rechte und für die Zusammenarbeit mit den Aufsichtsbehörden der Mitgliedstaaten zuständig sind, und

c) die von dem betreffenden Drittland bzw. der betreffenden internationalen Organisation eingegangenen internationalen Verpflichtungen oder andere Verpflichtungen, die sich aus rechtsverbindlichen Übereinkünften oder Instrumenten sowie aus der Teilnahme des Drittlands oder der internationalen Organisation an multilateralen oder regionalen Systemen insbesondere in Bezug auf den Schutz personenbezogener Daten ergeben.

(3) Nach der Beurteilung der Angemessenheit des Schutzniveaus kann die Kommission im Wege eines Durchführungsrechtsaktes beschließen, dass ein Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in einem Drittland oder eine internationale Organisation ein angemessenes Schutzniveau im Sinne des Absatzes 2 des vorliegenden Artikels bieten. In dem Durchführungsrechtsakt ist ein Mechanismus für eine regelmäßige Überprüfung, die mindestens alle vier Jahre erfolgt, vorzusehen, bei der allen maßgeblichen Entwicklungen in dem Drittland oder bei der internationalen Organisation Rechnung getragen wird. Im Durchführungsrechtsakt werden der territoriale und der sektorale Anwendungsbereich sowie gegebenenfalls die in Absatz 2 Buchstabe b des vorliegenden Artikels genannte Aufsichtsbehörde bzw. genannten Aufsichtsbehörden angegeben. Der Durchführungsrechtsakt wird gemäß dem in Artikel 93 Absatz 2 genannten Prüfverfahren erlassen.

Art. 46 DSGVO – Datenübermittlung vorbehaltlich geeigneter Garantien – lautet auszugsweise:

(1) Falls kein Beschluss nach Artikel 45 Absatz 3 vorliegt, darf ein Verantwortlicher oder ein Auftragsverarbeiter personenbezogene Daten an ein Drittland oder eine internationale Organisation nur übermitteln, sofern der Verantwortliche oder der Auftragsverarbeiter geeignete Garantien vorgesehen hat und sofern den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen.

(2) Die in Absatz 1 genannten geeigneten Garantien können, ohne dass hierzu eine besondere Genehmigung einer Aufsichtsbehörde erforderlich wäre, bestehen in

a) einem rechtlich bindenden und durchsetzbaren Dokument zwischen den Behörden oder öffentlichen Stellen,

b) verbindlichen internen Datenschutzvorschriften gemäß Artikel 47,

c) Standarddatenschutzklauseln, die von der Kommission gemäß dem Prüfverfahren nach Artikel 93 Absatz 2 erlassen werden,

d) von einer Aufsichtsbehörde angenommenen Standarddatenschutzklauseln, die von der Kommission gemäß dem Prüfverfahren nach Artikel 93 Absatz 2 genehmigt wurden,

e) genehmigten Verhaltensregeln gemäß Artikel 40 zusammen mit rechtsverbindlichen und durchsetzbaren Verpflichtungen des Verantwortlichen oder des Auftragsverarbeiters in dem Drittland zur Anwendung der geeigneten Garantien, einschließlich in Bezug auf die Rechte der betroffenen Personen, oder

f) einem genehmigten Zertifizierungsmechanismus gemäß Artikel 42 zusammen mit rechtsverbindlichen und durchsetzbaren Verpflichtungen des Verantwortlichen oder des Auftragsverarbeiters in dem Drittland zur Anwendung der geeigneten Garantien, einschließlich in Bezug auf die Rechte der betroffenen Personen.

Art. 7 Charta der Grundrechte der Europäischen Union – Achtung des Privat und Familienlebens – lautet:

Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation.

Art. 8 Charta der Grundrechte der Europäischen Union – Schutz personenbezogener Daten – lautet:

Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten. Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken. Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

Art. 47 Charta der Grundrechte der Europäischen Union – Recht auf wirksamen Rechtsbehelf und ein unparteiisches Gericht – lautet:

Jede Person, deren durch das Recht der Union garantierte Rechte oder Freiheiten verletzt worden sind, hat das Recht, nach Maßgabe der in diesem Artikel vorgesehenen Bedingungen bei einem Gericht einen wirksamen Rechtsbehelf einzulegen. Jede Person hat ein Recht darauf, dass ihre Sache von einem unabhängigen, unparteiischen und zuvor durch Gesetz errichteten Gericht in einem fairen Verfahren, öffentlich und innerhalb angemessener Frist verhandelt wird. Jede Person kann sich beraten, verteidigen und vertreten lassen. Personen, die nicht über ausreichende Mittel verfügen, wird Prozesskostenhilfe bewilligt, soweit diese Hilfe erforderlich ist, um den Zugang zu den Gerichten wirksam zu gewährleisten.

Erwägungsgrund 26 der DSGVO – Keine Anwendung auf anonymisierte Daten – lautet:

[1]Die Grundsätze des Datenschutzes sollten für alle Informationen gelten, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. [2]Einer Pseudonymisierung unterzogene personenbezogene Daten, die durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden könnten, sollten als Informationen über eine identifizierbare natürliche Person betrachtet werden. [3]Um festzustellen, ob eine natürliche

Person identifizierbar ist, sollten 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. [4]Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind. [5]Die Grundsätze des Datenschutzes sollten daher nicht für anonyme Informationen gelten, d.h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann. [6]Diese Verordnung betrifft somit nicht die Verarbeitung solcher anonymer Daten, auch für statistische oder für Forschungszwecke.

Erwägungsgrund 30 der DSGVO – Online-Kennungen zur Profilerstellung und Identifizierung – lautet:

[1]Natürlichen Personen werden unter Umständen Online-Kennungen wie IP-Adressen und Cookie-Kennungen, die sein Gerät oder Software-Anwendungen und -Tools oder Protokolle liefern, oder sonstige Kennungen wie Funkfrequenzkennzeichnungen zugeordnet. [2]Dies kann Spuren hinterlassen, die insbesondere in Kombination mit eindeutigen Kennungen und anderen beim Server eingehenden Informationen dazu benutzt werden können, um Profile der natürlichen Personen zu erstellen und sie zu identifizieren.

II.3.3. Zum Anwendungsbereich der Art. 44 ff DSGVO:

Soweit die folgenden drei Voraussetzungen erfüllt sind, liegt eine Übermittlung vor und Kapitel V (Art. 44 ff) DSGVO ist anwendbar (Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPr, Version 2.0, angenommen am, 14.02.2023):

1) Ein für die Verarbeitung Verantwortlicher oder ein Auftragsverarbeiter ("Exporteur") unterliegt bei der jeweiligen Verarbeitung der DSGVO.

2) Der Exporteur übermittelt personenbezogene Daten, die Gegenstand dieser Verarbeitung sind, an einen anderen für die Verarbeitung Verantwortlichen, einen gemeinsam für die Verarbeitung Verantwortlichen oder einen Auftragsverarbeiter ("Importeur") oder stellt sie auf andere Weise zur Verfügung.

3) Der Importeur befindet sich in einem Drittland, unabhängig davon, ob dieser Importeur für die jeweilige Verarbeitung gemäß Artikel 3 der DSGVO unterliegt oder eine internationale Organisation ist.

Aus Art. 8 Abs. 1 EU-GRC ergibt sich eine Pflicht zur Perpetuierung des unionsrechtlichen Schutzniveaus (EuGH 06.10.2015, C-362/14 *(Schrems)*, Rn 72). Die gegenständlichen

Bestimmungen regeln die Bedingungen, welche es einem Verantwortlichen oder Auftragsverarbeiter (Exporteur) erlauben, personenbezogene Daten in ein Drittland zu übermitteln. Der nicht legaldefinierte Begriff der Übermittlung ist im Rahmen der Art. 44 ff schutzzweckbezogen zu verstehen. Er umfasst daher jede Weitergabe von personenbezogenen Daten an eine Stelle außerhalb des Territoriums der Europäischen Union oder an eine internationale Organisation (*Kühling/Buchner*, DSGVO·BDSG[3], Art. 44, Rn 16, *Jahnel*, Kommentar zur Datenschutz-Grundverordnung Art. 44 DSGVO (Stand 1.12.2020, rdb.at), Rn 18). Aus Art. 44 DSGVO ergibt sich, dass der Importeur (Empfänger im Drittland) nicht vom Anwendungsbereich der Norm erfasst ist, weil dieser gerade nicht die Übermittlung von Daten veranlasst. Der Begriff „Übermittlung" beschreibt eine Handlung des Datenexporteurs, nicht aber eine Handlung des Datenimporteurs. Ferner bestimmt Art. 46 Abs. 1 DSGVO, dass ein Verantwortlicher oder ein Auftragsverarbeiter personenbezogene Daten an ein Drittland oder eine internationale Organisation nur übermitteln darf, sofern der Verantwortliche oder der Auftragsverarbeiter geeignete Garantien vorgesehen hat und sofern den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen. Im Ergebnis stellt der klare Wortlaut der Art. 44 ff DSGVO keine unmittelbaren Anforderungen an Datenimporteure (so auch richtigerweise die BF2, VWA ./43, Seite 19). Aufgrund der Rechtsprechung des Europäischen Gerichtshofes trägt der Datenexporteur die Verantwortung für die Prüfung der Zulässigkeit der konkreten Übermittlung. Er muss jederzeit von sich aus prüfen, ob die Daten im Drittland geschützt sind (*Kühling/Buchner*, DSGVO·BDSG[3], Art. 44, Rn 16 mit Verweis auf EuGH 16.07.2020, C-311/18 *(Schrems II)*). Insgesamt sind aus Kapitel V DSGVO keine subjektiven öffentliche Rechte/Pflichten für einen Datenimporteur zu entnehmen.

Davon abzugrenzen sind zum Beispiel vertragliche Pflichten eines Datenimporteurs, zum Beispiel, dass er den Datenexporteur unverzüglich darüber informieren muss, wenn das für ihn anwendbare Recht es ihm nicht mehr erlaubt, die Daten in Übereinstimmung mit den Sondervertragsklauseln zu speichern und zu verarbeiten (Beschluss der Kommission vom 05.02.2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates (2010/87/EU), Klausel 5 – Pflichten des Datenimporteurs). Diese sind jedoch nicht Gegenstand eines verwaltungsbehördlichen/-gerichtlichen Verfahrens.

II.3.4. Zu Art. 44 DSGVO als subjektives Recht:

Wiederholend führte die BF2 im Verfahren aus, dass eine Verletzung der Art. 44 ff DSGVO kein zulässiger Gegenstand einer Beschwerde gemäß Art 77 DSGVO sei (VWA ./54, Seite 6, VWA ./62, Seite 36). Dieser Ansicht ist aus folgenden Gründen nicht zu folgen:

§ 24 DSG räumt der in seinem persönlichen Grundrecht verletzten Person die Möglichkeit ein, die ihr gegenüber geschehene Rechtsverletzung feststellen zu lassen. Der Feststellungsausspruch betrifft hier die Rechtsposition einer konkreten in ihren Rechten verletzten Person und ist dogmatisch in seinem Rechtskraftumfang auf diese Rechtsverletzung beschränkt. Basierend auf dieser Feststellung soll es der betroffenen Person möglich sein, weitere individuelle Ansprüche – etwa Schadenersatzansprüche – zu verfolgen (VwGH 14.12.2021, Ro 2020/04/0032).

Eine Abhängigkeit dahingehend, dass die Datenschutzbehörde nur dann eine Rechtsverletzung feststellen darf, wenn der Betroffene ein Betroffenenrecht (Art 12 ff DSGVO) geltend macht, kann aus § 24 DSG nicht gewonnen werden. Im Zusammenhang mit Art. 77 DSGVO ergibt sich eine Entscheidungspflicht der Datenschutzbehörde, wenn die betroffene Person der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen diese Verordnung verstößt. Entgegen der Ansicht der BF2 ist jedoch Art. 77 DSGVO eine Einschränkung auf Betroffenenrechte gemäß Art. 12 ff DSGVO nicht zu entnehmen (so zB VWA ./43, Seite 17). Eine betroffene Person kann eine Rechtsverletzung dem Grunde nach auf jede Bestimmung der DSGVO stützen, sofern die DSGVO-widrige Verarbeitung personenbezogener Daten auch zu einer Verletzung der Rechtsposition der betroffenen Person führt (so auch die überwiegende Lehre: *Jahnel*, Kommentar zur Datenschutz-Grundverordnung Art. 77 DSGVO (Stand 1.12.2020, rdb.at), Rn 11; *Bergt* in *Kühling/Buchner*, DSGVO·BDSG[3], Art. 77, Rn 10; *Körffer* in *Paal/Pauly*, Datenschutzgrundverordnung·Bundesdatenschutzgesetz[3], Art. 77; *Moos/Schefzig* in *Taeger/Gabel*, DSGVO·BDSG·TTDSG[4], Art. 77, Rn 9; *Boehm* in *Simitis|Hornung|Spiecker*, Datenschutzrecht, Art. 77, Rn 6). In § 24 DSG sollen im Rahmen der Durchführung des Art. 77 DSGVO das Recht auf Beschwerde bei einer Aufsichtsbehörde sowie die Grundsätze des Verfahrens vor der Aufsichtsbehörde geregelt werden (1761 BlgNR 25. GP 15). Aus den Materialien wird eindeutig erkennbar, dass mit § 24 DSG das Recht eines Betroffenen auf Beschwerde bei einer Aufsichtsbehörde nach Art. 77 DSGVO näher konkretisiert wird. Den Materialien ist nicht zu entnehmen, dass mit § 24 DSG der Umfang der Beschwerderechte eines Betroffenen eingeschränkt wird.

Gemäß § 24 Abs. 1 DSG hat jede betroffene Person das Recht auf Beschwerde bei der Datenschutzbehörde, wenn sie der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten – (ua.), gemeint unter anderem – gegen § 1 DSG, der auch das Recht auf Geheimhaltung schützt, verstößt. Gemäß § 24 Abs. 2 Z 5 DSG hat die Beschwerde das Begehren zu enthalten, die behauptete Rechtsverletzung festzustellen. Soweit sich eine Beschwerde als berechtigt erweist, ist ihr nach § 24 Abs. 5 erster Satz DSG Folge zu geben. Das Gesetz sieht demnach als Rechtsbehelf im Fall einer datenschutzrechtlichen Rechtsverletzung

explizit einen Feststellungsantrag im Rahmen der Beschwerde vor, der gemäß § 24 Abs. 5 DSG Folge zu geben ist, sofern sie sich als berechtigt erweist (VwGH 19.10.2022, Ro 2022/04/0001).

Ist daher eine Person der Ansicht, dass die Verarbeitung der sie betreffenden personenbezogenen Daten zu einer Verletzung ihrer Rechte führt, so hat sie gemäß § 24 DSG einen ausdrücklich im Gesetz vorgesehenen Anspruch, dies festzustellen zu lassen. In diesem Zusammenhang ist zu beachten, dass nicht nur eine Feststellung einer Rechtsverletzung gemäß § 1 DSG (Recht auf Geheimhaltung) möglich ist. Mit dem Ausdruck „unter anderem" gibt der Verwaltungsgerichtshof eindeutig zu verstehen, dass nicht nur Rechtsverletzungen festgestellt werden können, die auf § 1 DSG (Recht auf Geheimhaltung) basieren. Auch § 24 Abs. 2 DSG ist keine Einschränkung dahingehend zu entnehmen, dass eine betroffene Person nur eine Feststellung einer Verletzung des Rechts auf Geheimhaltung beantragen könnte.

Verfahrensgegenständlich zeigte der BF1 eine Rechtsverletzung gemäß § 24 Abs. 2 DSG dahingehend auf, dass die Verarbeitung seiner personenbezogenen Daten gegen die DSGVO verstößt (Art. 77 DSGVO). Konkret begehrte der BF1 eine Feststellung, ob eine Verletzung der allgemeinen Grundsätze der Datenübermittlung gemäß Art. 44 DSGVO erfolgte.

Zweifelsfrei hat jede Person das subjektive Recht, sofern ihre personenbezogenen Daten von anderen verarbeitet werden, dass die Verarbeitung der personenbezogenen Daten des Betroffenen im Einklang der DSGVO erfolgt. Entsprechend der Rechtsprechung des Europäischen Gerichtshofes muss jede Verarbeitung personenbezogener Daten zum einen mit den in Art. 5 der DSGVO aufgestellten Grundsätzen für die Verarbeitung der Daten im Einklang stehen und zum anderen einem der in Art. 6 der DSGVO anfgeführten Grundsätze in Bezug auf die Rechtmäßigkeit der Verarbeitung entsprechen (EuGH 22.06.2021, C-439/19 *(Latvijas Republikas Saeima)*, Rn 96). Soweit eine betroffene Person der Ansicht ist, dass die Verarbeitung von personenbezogenen Daten nicht der DSGVO entspricht, so ist dahingehend eine Individualbeschwerde gemäß § 24 DSG zulässig.

Verfahrensgegenständlich ist besonders hervorzuheben, dass der Europäische Gerichtshof (EuGH 16.07.2020, C-311/18 *(Schrems II)*, Rn 158) davon ausgegangen ist, 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. In diesem Zusammenhang führte die bB zutreffend aus, 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 (VWA ./59, Seite 23 f).

Insgesamt ist die bB befugt, eine Rechtsverletzung nach Art. 44 ff DSGVO feststellen.

II.3.5. Zur Rollenverteilung:

Die MB hat zum verfahrensgegenständlichen Zeitpunkt als Website-Besitzerin die Entscheidung getroffen das Tool „ XXXX -Analytics“ auf der Website XXXX zu implementieren. Konkret hat sie einen JavaScript Code („tag“), der seitens der BF2 zur Verfügung gestellt wird, im Quelltext ihrer Website eingefügt, wodurch dieser JavaScript Code beim Besuch der Website im Browser des BF1 ausgeführt wurde. Die MB hat das genannte Tool zum Zwecke von statistischen Auswertungen über das Verhalten der Websitebesucher eingesetzt. Da die MB über die Zwecke und die Mittel der mit dem Tool in Verbindung stehenden Datenverarbeitung entschieden hat, ist sie als Verantwortliche iSd Art. 4 Z 7 DSGVO anzusehen.

Verfahrensgegenständlich ist zu beachten, dass der Beschwerdegegenstand sich nur auf die Datenübermittlung an die BF2 (Vereinigte Staaten) bezieht. Im Zusammenhang mit der Datenübermittlung mit dem Tool XXXX -Analytics ist zu beachten, dass die BF2 das Tool nur zur Verfügung stellt und darauf keinen Einfluss hat, ob es überhaupt bzw. inwiefern die MB von den Toolfunktionen Gebrauch macht und welche konkreten Einstellungen sie wählt. Soweit die BF2 XXXX -Analytics (als Dienstleistung) nur bereitstellt, nimmt sie keinen Einfluss auf „Zwecke und Mittel“ der Datenverarbeitung und ist daher iSd Art. 4 Z 8 DSGVO fallbezogen als Auftragsverarbeiter zu qualifizieren.

II.3.6. Zu Spruchpunkt A.I) – Zurückweisung der Bescheidbeschwerde der BF2:

II.3.6.1. Zur Beschwerdelegitimation der BF2:

Mit Hilfe der Feststellungen im Spruchpunkt 2. im verfahrensgegenständlichen Bescheid wird geklärt, ob eine Verletzung der allgemeinen Grundsätze der Datenübermittlung gemäß Art. 44 DSGVO durch die MB vorliegt. Der Spruchpunkt 2. ist gemäß § 59 Abs. 1 AVG von den übrigen Spruchpunkten trennbar, weil er für sich allein ohne einen inneren Zusammenhang mit anderen Teilen des Verfahrens einem gesonderten Abspruch zugänglich ist (vgl. etwa VwGH 12.9.2018, Ra 2015/08/0032). Zutreffend führte die bB aus, dass die mögliche Verletzung von Art. 5 ff iVm Art. 38 Abs. 3 lit. a und Art. 29 DSGVO durch die BF2 in keinem Zusammenhang mit den Vorgaben von Art. 44 DSGVO steht (VWA ./67, Seite 14).

Die Frage, wer in einem konkreten Verwaltungsverfahren Parteistellung besitzt, kann anhand des AVG alleine nicht gelöst werden. Die Parteistellung muss vielmehr aus den materiellrechtlichen Vorschriften abgeleitet werden. Auf dem Boden des materiellen Verwaltungsrechts muss sie nach dem Gegenstand des betreffenden Verwaltungsverfahrens und nach dem Inhalt der zur Anwendung kommenden Verwaltungsvorschriften beurteilt werden. Das Tatbestandsmerkmal der Parteistellung in Verwaltungsangelegenheiten bestimmt sich demnach nach dem normativen Gehalt der in der Rechtssache anzuwendenden Vorschriften. Die Begriffe "Rechtsanspruch" und "rechtliches Interesse" gewinnen erst durch die jeweils zur Anwendung kommende Verwaltungsvorschrift an einem konkreten Inhalt, wonach allein die Frage der Parteistellung beantwortet werden kann (VwGH 19.04.2022, Ra 2021/02/0251). Vor diesem Hintergrund kann eine Parteistellung im verwaltungsgerichtlichen Verfahren nicht damit begründet werden, weil sich Verfahrensergebnisse sich auf ein anderes Verfahren auswirken können; die Parteistellung (bzw. rechtliche Interessen) leitet sich vielmehr von der maßgeblichen Verwaltungsvorschrift ab, die Gegenstand des verwaltungsbehördlichen Verfahrens waren.

Wie unter Punkt II.3.3 ausgeführt, regelt Art. 44 DSGVO die Zulässigkeit einer Datenübermittlung in ein Drittland. Aufgrund der Rechtsprechung des Europäischen Gerichtshofes trägt der Datenexporteur (die MB) die Verantwortung für die Prüfung der Zulässigkeit der konkreten Übermittlung. Er muss jederzeit von sich aus prüfen, ob die Daten im Drittland geschützt sind. Vor diesem Hintergrund ist eindeutig erkennbar, dass die Regelungen in Kapitel V DSGVO ausnahmslos subjektive öffentliche Rechte/Pflichten des Datenexporteurs (sohin der MB) zum Gegenstand haben. Demgegenüber sind subjektive öffentliche Rechte/Pflichten für den Datenimporteur in einem Drittland aus Kapitel V DSGVO nicht zu entnehmen. Dies wird auch daran erkennbar, dass für die Beurteilung der Rechtsfrage, ob ein Datenexporteur Pflichten gemäß Kapitel V DSGVO verletzt hat, grundsätzlich eine Teilnahme des Datenimporteurs im Verfahren nicht erforderlich ist. Ist daher ein Datenimporteur beispielsweise für eine Aufsichtsbehörde überhaupt nicht erreichbar, so hindert dieser Umstand die Aufsichtsbehörde nicht daran, allenfalls eine Rechtsverletzung des Datenexporteurs gemäß Kapitel V DSGVO festzustellen. Im Ergebnis kam daher der BF2 im Zusammenhang mit der Beurteilung der Rechtsfrage, ob der Datenexporteur (also die MB) Pflichten nach Kapitel V DSGVO verletzt hat, im Verfahren der bB (VWA ./59, Spruchpunkt 2) keine Parteistellung zu.

In Spruchpunkt 3 des verfahrensgegenständlichen Bescheides war die BF2 Partei im Verfahren, da die bB die Rechtsfrage klärte, ob die BF2 gegen Pflichten gemäß Art. 44 DSGVO verstoßen hat. Da jedoch Art. 44 bzw. Kapitel V DSGVO keine öffentlich-rechtlichen

Verpflichtungen für einen Datenimporteur in einem Drittland vorsieht, hat die bB ein dahingehendes Begehren des BF1 abgewiesen. Die bB bestätigte dahingehend die Rechtsansicht der BF2 (siehe oben Punkt II.3.3).

Wie dargelegt, kam der BF2 im Zusammenhang mit Spruchpunkt 2 im Verfahren der bB keine Parteienstellung zu. Diese Parteienstellung im verwaltungsbehördlichen Verfahren ist jedoch unabdingbare Voraussetzung für die Erhebung einer Bescheidbeschwerde an ein Verwaltungsgericht. Die Parteistellung im Verwaltungsverfahren und die Befugnis zur Beschwerdeerhebung hängen nach der innerstaatlichen Rechtslage unmittelbar zusammen (VwGH 05.04.2022, Ra 2022/03/0073). Da der BF2 im Verwaltungsverfahren zu Spruchpunkt 2. des verfahrensgegenständlichen Bescheides keine Parteistellung zukam, war ihre Bescheidbeschwerde dahingehend zurückzuweisen.

Weiters wird darauf hingewiesen, dass eine vorfragenweise Beurteilung in Bescheiden ganz allgemein keine Bindungswirkung für andere Behörden (oder auch dieselbe Behörde in einem anderen Verfahren) entfaltet, für deren Entscheidung dieselbe Frage oder aber eine inhaltlich vergleichbare (wenngleich nicht als Vorfrage im rechtlichen Sinn zu qualifizierende) Frage von Bedeutung ist (VwGH 20.01.2016, Ro 2014/04/0045). Zudem ist die Hauptfrage des verfahrensgegenständlichen Teilbescheides die Absprache hinsichtlich einer Verletzung von Art. 44 DSGVO, also die Frage, ob die verfahrensgegenständliche Datenübermittlung in ein Drittland rechtlich zulässig war. Hauptfrage sind jedoch nicht auch einzelne Feststellungen zu einigen Tatbestandselementen der Art. 44 ff DSGVO, welche im Spruchpunkt 2. ausgeführt sind.

Auch ist zu beachten, dass die BF2 als Auftragsverarbeiter für die MB agierte. Sohin waren ihre Handlungen der MB zuzurechnen (Art. 28 DSGVO), welche schließlich zu einer Rechtsverletzung durch die MB führten. In diesem Zusammenhang wird darauf hingewiesen, dass die MB gegen die Entscheidung der bB keine Bescheidbeschwerde erhob.

II.3.6.2. Zur fehlenden Verletzung von subjektiven Rechten der BF2:

Unabhängig von der fehlenden Parteistellung (siehe Punkt II.3.6.1) liegt, entgegen den Ausführungen der BF2 (VWA ./62, Seite 8), fallgegenständlich eine Verletzung von subjektiven Rechten schon im Grund nach nicht vor. Dies aus folgenden Erwägungen:

II.3.6.2.1. Zur Verarbeitung von personenbezogenen Daten:

Personenbezogene Daten sind gemäß Art. 2 Abs. 1 DSGVO Anknüpfungspunkt für die sachliche Anwendbarkeit der DSGVO. In diesem Zusammenhang hat der Europäische Gerichtshof wiederholt ausgesprochen, dass der Anwendungsbereich der DSGVO sehr weit zu verstehen ist (EuGH 22.06.2021, C-439/*19 (Latvijas Republikas Saeima)*, Rn 61; 20.12.2017, C-434/16

(Peter Nowak), Rn 59). Dieses grundlegende Verständnis ist den weiteren Ausführungen zugrunde zu legen. Vor diesem Hintergrund ist der Ansicht der bB zu folgen, dass ein Eingriff in das Grundrecht auf Datenschutz gemäß Art. 8 EU-GRC sowie § 1 DSG bereits dann vorliegt, wenn gewisse Maßnahmen gesetzt werden (zB Zuordnung von Kennnummern), um Website-Besucher zu individualisieren.

Im vorliegenden Fall indizieren bereits eigene Erklärungen sowie Verhaltensweisen der BF2, dass die verfahrensgegenständlichen übertragenden Informationen (siehe Punkt II.1.3.1) personenbezogene Daten darstellen. So erklärt die BF2 selbst, dass im Rahmen des Auftragsverarbeitungsdienstes „ XXXX Analytics“ die Daten „Online-Kennzeichnungen (einschließlich Cookie-Kennungen), Internet-Protokoll-Adressen und Gerätekennungen und vom Kunden vergebene Kennzeichnungen“ personenbezogene Daten sein können. Zudem setzte die BF nach dem Urteil des Europäischen Gerichtshofes vom 16.07.2020 in der Rechtssache C-311/18 mehrere Maßnahmen, um eine rechtskonforme Übertragung von personenbezogenen Daten in die Vereinigten Staaten (siehe Punkt II.1.9) zu ermöglichen. Diese Erklärungen bzw. Verhaltensweisen stehen den wenig überzeugenden Ausführungen der MB bzw. der BF2 entgegen, dass die Änderung der Auftragsdatenverarbeitungsbedingungen (DTPS) vom 12.08.2020 unter Einbeziehung der Standardvertragsklauseln (SCCs) nur aus proaktiven Gründen vorgenommen worden seien.

Grundsätzlich gilt zu beachten, dass aus den am 14.08.2020 übermittelten Informationen (siehe Punkt II.1.3 und II.1.3.1) ein unmittelbarer Personenbezug nicht zu entnehmen ist. Online-Kennungen (IP-Adresse, Cookies, etc.) identifizieren für sich allein genommen regelmäßig keine Person, da sich aus ihnen unmittelbar weder die Identität der natürlichen Person, der das Endgerät (Computer) gehört, von dem aus eine Website aufgerufen wurde, noch die Identität einer anderen Person, die diesen Computer benutzen könnte, ergibt (EuGH 19.10.2016, C-582/14 *(Breyer)*, Rn 38). Jedoch ist eine Identifizierbarkeit je nach Sachverhalt möglich.

Eine Information macht eine natürliche Person identifizierbar, wenn durch sie allein die Identifizierung (also die Wiedererkennung) zwar selbst nicht unmittelbar möglich ist, eine entsprechende Identifizierung aber mittels Verknüpfung mit weiteren Informationen hergestellt werden kann. Als identifizierbar wird nach Art. 4 Z 1 DSGVO eine 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, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann. Die Kenntnis des Namens der natürlichen

Person ist jedoch für eine Identifizierbarkeit nicht unbedingt erforderlich (Art.-29-Datenschutzgruppe, WP 136, Seite 16 f).

Um festzustellen, ob eine natürliche Person identifizierbar ist, sind alle Mittel zu berücksichtigen, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren (ErwG 26, 3. Satz). Die rein hypothetische Möglichkeit zur Identifizierung der Person reicht jedoch nicht aus, um die Person als identifizierbar anzusehen. Es ist allerdings auch nicht notwendig, dass der Verantwortliche tatsächlich Bestrebungen einleitet oder über entsprechende Mittel bereits verfügt, um eine Identifizierung herbeizuführen, sondern es reicht die Wahrscheinlichkeit, dass er diese einleitet bzw. entsprechende Mittel erwerben wird. Für die Beurteilung der Frage der Identifizierbarkeit kommt es daher nicht darauf an, ob ein Verantwortlicher tatsächlich einen Versuch unternommen hat, eine Identifizierung vorzunehmen. Es ist ausreichend, dass die Nutzung eines Mittels, unter rein abstrakt zu beurteilenden Gesichtspunkten wahrscheinlich ist.

Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sind im Rahmen einer Risikoanalyse bzw. -prognose (nach ErwG 26, 4. Satz) alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, heranzuziehen, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklung zu berücksichtigen sind. Entsprechend der Rechtsprechung des Europäischen Gerichtshofes ist hierfür ein faktisches Risiko der Herstellung eines Personenbezugs erforderlich (EuGH 19.10.2016, C-582/14 *(Breyer)*, Rn 38). Zur Bestimmung, ob ein solches Risiko gegeben ist, ist – neben den in ErwG 26, 3. Satz ausdrücklich genannten Faktoren – auch zu berücksichtigen, ob der Zweck der Verarbeitung eine Identifizierung erfordert, ob die Identifizierung zu einer Nutzungssteigerung führt und ob der Identifizierung vertragliche und/oder organisatorische Hemmnisse (zB Vertragsstrafen) entgegenstehen (*Taeger/Gabel*, DSGVO·BDSG·TTDSG[4], Art. 4, Rn 31). Im vorliegenden Fall ist schon deshalb von einer Nutzungssteigerung auszugehen, weil zB durch die verwendeten Online-Kennungen (IP-Adresse, Cookies) eine Unterscheidung von Website-Besuchern ermöglicht wird. Auch ist im Kontext von Big-Data-Anwendungen die Schwelle zur Annahme eines Personenbezugs schlicht niedrig (*Kühling/Buchner*, DSGVO·BDSG[3], Art. 4 Nr. 1, Rn 22). Hat zB ein Unternehmen in zwei unterschiedlichen Datenbanken Informationen über Personen gespeichert (die isoliert betrachtet jedoch keine eindeutige Zuordnung zu einer Person ermöglichen), deren Zusammenführung dabei zu einer Identifizierung führen würde und unter Berücksichtigung der typsicherweise am Markt verfügbaren Datenanalysetools mit einem vertretbaren Aufwand an Zeit und Kosten möglich

wäre, wäre die Identifizierbarkeit auch der (noch) nicht zusammengeführten Datenbanken zu bejahen (*Taeger/Gabel*, DSGVO·BDSG·TTDSG[4], Art. 4, Rn 31). Zudem wird auch 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. *Kargl* in *Simits/Hornung/Spiecker*, Datenschutzrecht, Art. 4 Z 1, Rn 52 mwN). Mit Hilfe des Fingerprintings (RFC6973) kann ein Beobachter ein Gerät oder eine Anwendungsinstanz mit ausreichender Wahrscheinlichkeit auf Grundlage mehrerer Informationselemente (Online-Kennungen, IP-Adresse, Browserinformationen, etc.) identifizieren.

Zudem ist der Argumentation der bB zu folgen, dass die Implementierung von XXXX -Analytics auf XXXX eine Aussonderung iSd ErwG 26 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 „allgemeinen Ermessen“ keine Mittel zu verwenden, um natürliche Personen identifizierbar zu machen. Es ist davon auszugehen, dass ohne Verwendung der verfahrensgegenständlichen Informationen (siehe Punkt II.1.3.1) die BF2 nicht in der Lage wäre, einen brauchbaren Messdienst (siehe Punkt II.1.4) anzubieten, weil bspw die BF2 ohne Cookies nicht in der Lage wäre, nachvollziehbare Messungen von Website-Besuchen durchzuführen.

Aufgrund der vorliegenden Umstände – Big Data, Nutzensteigerungen, des Zwecks und der Funktionsweise des Webanalysedienstes XXXX -Analytics und Fingerprinting – ist von einem faktischen Risiko auszugehen, dass die BF2 als Auftragsverarbeiterin der MB nach allgemeinem Ermessen wahrscheinlich Mittel zur Identifizierung der natürlichen Person einsetzt.

Mit den an die BF2 übermittelten Informationen (siehe Punkt II.2.3 bzw. II.2.3.1) wird ein „digitaler Fußabdruck“ des BF1 erzeugt, welcher es der BF2 als Auftragsverarbeiter der MB ermöglicht, den BF1 zu identifizieren.

Im Hinblick auf die Online-Kennungen ist zu beachten, dass die gegenständlichen Cookies „_ga“ bzw. „cid“ (Client ID) und “_gid” (User ID) einzigartige XXXX -Analytics Kennnummern enthalten und auf dem Endgerät bzw. im Browser des BF1 abgelegt wurden. Mit diesen Kennungen ist es der BF2 mitunter möglich, Website-Besucher zu unterscheiden und auch die Information zu erhalten, ob es sich um einen neuen oder um einen wiederkehrenden Website-Besucher von XXXX handelt. Ohne diese Kennnummern ist daher eine Unterscheidung von Website-Besuchern nicht möglich. In diesem Zusammenhang vertritt der Europäische Datenschutzbeauftragte die Ansicht, dass alle Datensätze, die Identifizierungsmerkmale enthalten, mit denen Nutzer ausgesondert werden können, nach der Verordnung (gemeint

Verordnung (EU) 2018/1725) als personenbezogene Daten gelten und als solche behandelt geschützt werden müssen (VWA ./68).

Hinsichtlich der IP-Adresse ist zu beachten, dass die „Anonymisierungsfunktion“ der IP-Adresse im Zeitpunkt der Datenübertragung an die BF2 nicht korrekt implementiert wurde und daher von der BF2 vollständig gespeichert wurde. In diesem Zusammenhang ist zu beachten, dass die allgemeine Speicherung der IP-Adressen einen schweren Eingriff in die in den Art. 7 und 8 der Charta verankerten Grundrechte darstellt, da es mit IP-Adressen möglich ist, genaue Schlüsse auf das Privatleben des Nutzers des betreffenden elektronischen Kommunikationsmittels zu ziehen. Dies kann eine abschreckende Wirkung in Bezug auf die Ausübung der in Art. 11 der Charta garantierten Freiheit der Meinungsäußerung haben (EuGH 20.09.2022 in den verbundenen Rechtssachen C-793/19 und C-794/19 *(SpaceNet AG/Telekom Deutschland GmbH)*, Rn 100). Auch spielt keine Rolle, wem eine IP-Adresse tatsächlich gehört: Entscheidend ist der Umstand, ob von der IP-Adresse Rückschlüsse auf die betroffene Person (Nutzer) gezogen werden können. Daher kommt den Ausführungen der BF2 kein Begründungswert zu, wenn sie die Auffassung vertritt, dass die verwendete IP-Adresse möglicherweise dem Arbeitgeber des BF1 gehört. Unabhängig davon hat das Verfahren ergeben, dass die IP-Adresse des BF1 unmittelbar an die BF2 übermittelt wurde.

Schon aus der Kombination der übermittelten Informationen (siehe Punkt II.1.3.1) – Online-Kennungen, IP-Adresse, Informationen zum Browser, Betriebssystem, Bildschirmauflösung, Sprachauswahl, usw. – kann ein „digitaler Fußabdruck“ generiert werden, der es erlaubt, dass Endgerät und in weiterer Folge den konkreten Nutzer eindeutig zu individualisieren. Unabhängig davon ist im vorliegenden Fall für die BF2 als Auftragsverarbeiter eine Rückführbarkeit auf den BF1 möglich:

So war der BF1 im Zeitpunkt des Besuchs der Website XXXX auf seinem XXXX -Account XXXX eingeloggt. Die BF2 hat ausgeführt, dass sie aufgrund des Umstands, dass das Tool XXXX -Analytics auf einer Website implementiert ist, Informationen erhält. Hierzu zählt die Information, dass ein bestimmter XXXX -Account-Nutzer eine gewisse Website besucht hat (VWA ./31, Frage 9). In diesem Zusammenhang führte die BF2 aus, dass dies nur bei Aktivierung von spezifischen Einstellungen im XXXX -Account möglich sei (Aktivierung von „Personalisierte Werbung“ sowie von „Web- und App-Aktivitäten“ durch den XXXX -Account-Nutzer und Aktivierung von XXXX -Signals auf der Ziel-Website). Dazu führte die bB nachvollziehbar aus, dass die Identifizierbarkeit eines Website-Besuchers nicht davon abhängen könne, ob gewisse Willenserklärungen im XXXX -Account abgegeben werden, da aus technischer Sicht trotzdem alle Möglichkeiten für eine Identifizierung vorliegen würden. Anderseits könnte die BF2 den in den Kontoeinstellungen ausgedrückten Wünschen eines

Nutzers nach Personalisierung der erhaltenen Werbeinformationen nicht entsprechen. Dahingehend ist zu berücksichtigen, dass Art. 4 Z 1 DSGVO an ein „Können“ anknüpft („identifiziert werden kann“) und nicht daran, ob eine Identifizierung letztlich auch vorgenommen wird.

Unabhängig davon ist zu beachten, dass aus gewissen Einstellungen in einem XXXX -Konto bzw. durch die Aktivierung von XXXX -Signals auf einer Website bloß eine Anpassung an die persönlichen Bedürfnisse von Nutzern von XXXX -Anwendungen erfolgt. Die Anpassungen durch die Nutzer geben jedoch keine Rückschlüsse auf die Verarbeitung von Metainformationen durch die BF2, die im Zuge eines Aufrufes einer Anwendung (XXXX -Analytics, XXXX -Konto, XXXX , etc) an die BF2 übermittelt werden. Im Verfahren ist in diesem Zusammenhang eine Verknüpfung von Metainformationen und IP-Adresse zwischen XXXX -Konto und XXXX -Analytics hervorgekommen, welche einen unstrittigen Personenbezug ermöglichte.

Unabhängig von der BF2 besteht das faktische Risiko, dass US-Behörden nach allgemeinem Ermessen wahrscheinlich Mittel zur Identifizierung des BF1 einsetzen. In diesem Zusammenhang führte der BF1 nachvollziehbar aus, dass Nachrichtendienste der USA Online-Kennungen (IP-Adresse oder einzigartige Kennnummern) als Ausgangspunkt für die Überwachung von Einzelpersonen heranziehen. So kann insbesondere nicht ausgeschlossen werden, dass diese Nachrichtendienste bereits Informationen gesammelt haben, mit deren Hilfe die hier übertragenen Daten auf die Person des BF1 rückführbar sind. So übermittelt die BF2 aufgrund von Datenanfragen Metadaten und Inhaltsdaten. Der Umstand, dass es sich hierbei nicht bloß um eine „theoretische Gefahr“ handelt, zeigt sich am Urteil des Europäischen Gerichtshofes vom 16.07.2020, C-311/18 (*Schrems II*), 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. In diesem Zusammenhang haben weder der BF1 noch die MB die Möglichkeit zu verifizieren, ob US-Behörden bereits personenbezogene Daten übermittelt worden sind, bzw. ob US-Behörden bereits personenbezogene Daten des BF1 besitzen. Dieser Umstand kann der betroffenen Personen, wie dem BF1, nicht zur Last gelegt werden. So waren es letztlich die MB bzw. auch die BF2, die trotz Veröffentlichung des genannten Urteils des Europäischen Gerichtshofes vom 16.07.2020 das Tool XXXX -Analytics weiterhin eingesetzt haben. Schließlich ist auch der Argumentation der bB zu folgen, dass die MB einer Rechenschaftspflicht unterliegt (Art. 5 Abs. 2 iVm Art. 24 Abs. 1 iVm Art. 28 Abs. 1 DSGVO), dass die Verarbeitung gemäß der Verordnung erfolgte. In diesem Zusammenhang hat die MB ihrer Auftragsverarbeiterin (BF2) im Verfahren

keine organisatorischen bzw. technischen Maßnahmen aufgezeigt, welche geeignet sind, Methoden und Zugriffsmöglichkeiten der US-Behörden zu verhindern, damit es zu keiner Verletzung des Grundrechts auf Datenschutz gemäß Art. 8 EU-GRC kommen kann.

Im Ergebnis stellen die übermittelten Informationen (siehe Punkt II.1.3 bzw. II.1.3.1) jedenfalls in Kombination personenbezogene Daten gemäß Art. 4 Z 1 DSGVO dar.

II.3.6.2.2. Zum fehlenden angemessenen Schutzniveau gemäß Art. 44 DSGVO:

Art. 44 DSGVO sieht als Grundsatzbestimmung für den internationalen Datentransfer eine zweistufige Zulässigkeitsprüfung vor. Die erste Voraussetzung, dass Daten überhaupt in ein Drittland übermittelt werden dürfen, besteht darin, dass auch die sonstigen Bestimmungen der DSGVO (wie etwa Art. 5 f, Art. 13 f DSGVO) eingehalten werden. Im Rahmen der zweiten Stufe ist zu prüfen, ob eine der Voraussetzungen der Art. 45 – 49 DSGVO vorliegt. Der erste in Frage kommende Zulässigkeitstatbestand liegt nach Art. 45 DSGVO dann vor, wenn die Kommission für das betroffene Drittland in einem 1. Angemessenheitsbeschluss festgestellt hat, dass dieses ein angemessenes Schutzniveau bietet. Liegt ein derartiger Angemessenheitsbeschluss vor, bedarf es keiner Genehmigung für eine Datenübermittlung in das jeweilige Drittland. Besteht kein Angemessenheitsbeschluss, ist weiter zu prüfen, ob die Voraussetzungen nach Art. 46, 47 oder 49 DSGVO erfüllt sind.

Nachdem der Europäische Gerichtshof das „EU-US Privacy Shield“ mit der Entscheidung vom 16.07.2020, C-311/18 (*Schrems II*) für ungültig erklärt hat, kann die verfahrensgegenständliche Datenübertragung am 14.08.2020 (siehe Punkt II.1.3 bzw. II.1.3.1) auf der Grundlage eines Angemessenheitsbeschlusses nicht mehr begründet werden. Mit der Entscheidung des Europäischen Gerichtshofes wurde klargestellt, dass die Vereinigten Staaten bis auf weiteres als „Drittland“ anzusehen sind und derzeit eine Privilegierung für die Übermittlung von personenbezogenen Daten gemäß Art. 45 DSGVO nicht besteht.

Da ein Angemessenheitsbeschluss nach Art. 45 Abs. 3 DSGVO nicht besteht, sieht Art. 46 DSGVO weitere Zulässigkeitstatbestände („geeignete Garantien“) vor. Liegt eine der 2. in Art. 46 Abs. 2 DSGVO aufgezählten Garantien vor, ist der internationale Datenverkehr genehmigungsfrei zulässig. Die Garantien des Art. 3 DSGVO bestehen vorbehaltlich einer Genehmigung durch die zuständige Aufsichtsbehörde. Liegen keine der in Art. 46 Abs. 2 und Abs. 3 DSGVO aufgezählten Garantien vor, ist weiter zu prüfen, ob einer der 3. Ausnahmetatbestände für eine zulässige Drittlandübermittlung nach Art. 49 DSGVO erfüllt ist.

Verfahrensgegenständlich stützte die MB die Übertragung auf Standarddatenschutzklauseln gemäß Art. 46 Abs. 2 lit. c DSGVO. Auf weitere „geeignete Garantien“ gemäß Art. 46 DSGVO wurde die Übertragung der verfahrensgegenständlichen Daten von der MB nicht gestützt.

Daher wird in der Folge die Zulässigkeit der Datenübertragung gemäß Art. 46 Abs. 2 lit. c DSGVO untersucht.

II.3.6.2.2.1. Zur Datenübertragung auf Grundlage von Standarddatenschutzklauseln gemäß Art. 46 Abs. 2 lit. c DSGVO:

Die MB und die BF2 haben am 12.08.2020 gemäß Art. 46 Abs. 2 lit. c DSGVO Standarddatenschutzklauseln für die Übermittlung personenbezogener Daten in die Vereinigten Staaten abgeschlossen. („ XXXX Ads Data Processing Terms: Model Contract Clauses, Standard Contractual Clauses for Processors"). Konkret handelte es sich zum beschwerdegegenständlichen Zeitpunkt um jene Klauseln in der Fassung des Durchführungsbeschlusses der Europäischen Kommission 2010/87/EU vom 5. Februar 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates, ABl. L 2010/39, S. 5.

Bei der Übertragung von personenbezogenen Daten in ein Drittland müssen die Standarddatenschutzklauseln durchsetzbare Rechte und wirksamen Rechtsbehelfe gewährleisten, welche ein Schutzniveau genießen, das dem in der Union durch die DSGVO im Lichte der Charta garantierten Niveau der Sache nach gleichwertig ist. In diesem Zusammenhang sind insbesondere die vertraglichen Regelungen zu berücksichtigen, die zwischen dem in der Union ansässigen Verantwortlichen und dem im betreffenden Drittland ansässigen Empfänger der Übermittlung vereinbart wurden, sowie, was einen etwaigen Zugriff der Behörden dieses Drittlands auf die übermittelten personenbezogenen Daten betrifft, die maßgeblichen Elemente der Rechtsordnung dieses Landes, insbesondere die in Art. 45 Abs. 2 der DSGVO genannten Elemente (EuGH 16.07.2020, C-311/18 *(Schrems II)*, Rn 105). Die zuständige Aufsichtsbehörde ist verpflichtet, eine auf Standarddatenschutzklauseln gestützte Übermittlung personenbezogener Daten in ein Drittland auszusetzen oder zu verbieten, wenn diese Behörde im Lichte aller Umstände dieser Übermittlung der Auffassung ist, dass die Klauseln in diesem Drittland nicht eingehalten werden oder nicht eingehalten werden können und dass der nach dem Unionsrecht, insbesondere nach den Art. 45 und 46 der DSGVO sowie nach der Charta, erforderliche Schutz der übermittelten Daten nicht mit anderen Mitteln gewährleistet werden kann (EuGH 16.07.2020, C-311/18 *(Schrems II)*, Rn 121).

Im vorliegenden Fall ist zunächst zu beachten, dass der Europäische Gerichtshof das „EU-US Privacy Shield" deshalb für ungültig erklärt hat, da dieses mit den Art. 7, 8 und 47 der Charta unvereinbar war (EuGH 16.07.2020, C-311/18 *(Schrems II)*, Rn 150 ff), da es für US-Behörden (Nachrichtendienste) unverhältnismäßige Zugriffsmöglichkeiten bot und keine wirksamen

Rechtsbehelfe für Betroffene (nicht US-Bürger) zur Verfügung standen. So führte der Europäische Gerichtshof aus, dass betreffend der Art. 7 und 8 der Charta verbürgten Grundrechte weder Section 702 des FISA noch die E.O. 12333 in Verbindung mit der PPD-28 den im Unionsrecht nach dem Grundsatz der Verhältnismäßigkeit bestehenden Mindestanforderungen genügen, sodass nicht angenommen werden kann, dass die auf diese Vorschriften gestützten Überwachungsprogramme auf das zwingend erforderliche Maß beschränkt sind. Auch ist hinsichtlich der auf Section 702 des FISA gestützten als auch hinsichtlich der auf die E.O. 12333 gestützten Überwachungsprogramme zu beachten, dass weder die PPD-28 noch die E.O. 12333 den betroffenen Personen Rechte verleihen, die gegenüber den amerikanischen Behörden gerichtlich durchgesetzt werden können, sodass diese Personen nicht über einen wirksamen Rechtsbehelf verfügen. In diesem Zusammenhang bietet der im Angemessenheitsbeschluss genannte Ombudsmechanismus keinen Rechtsweg zu einem Organ, das den Personen, deren Daten in die Vereinigten Staaten übermittelt werden, Garantien böte, die den nach Art. 47 der Charta erforderlichen Garantien der Sache nach gleichwertig wären.

Diese Umstände, die zur Aufhebung des „EU-US Privacy Shield“ führten, sind auch bei der Beurteilung einer Datenübermittlung gemäß Art. 46 Abs. 2 lit. c DSGVO zu beachten. Dahingehend ist zu beachten, dass die Standarddatenschutzklauseln ihrer Natur nach keine Garantien bieten können, die über die vertragliche Verpflichtung, für die Einhaltung des unionsrechtlich verlangten Schutzniveaus zu sorgen, hinausgehen. Insbesondere können sie aufgrund des Vertragscharakters keine drittstaatlichen Behörden (wie US-Nachrichtendienste) binden (EuGH 16.07.2020, C-311/18 *(Schrems II)*, Rn 132 f).

Diese Überlegungen können auf den gegenständlichen Fall übertragen werden. So ist offenkundig, dass die BF2 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 die BF2 die Verpflichtung, den US-Behörden gemäß 50 U.S. Code § 1881a personenbezogene Daten zur Verfügung zu stellen. Die zwischen der MB und der BF2 vereinbarten Standarddatenklauseln bieten in diesem Zusammenhang keine Möglichkeiten, solchen Anforderungen wirksam zu begegnen bzw. solche zu verhindern. Wie sich aus dem Transparenzbericht der BF2 ergibt, werden auch regelmäßig derartige Anfragen von US-Behörden an sie gestellt.

Die gegenständliche Datenübermittlung kann daher nicht allein auf die zwischen der MB und der BF2 abgeschlossenen Standarddatenschutzklauseln gemäß Art. 46 Abs. 2 lit. c DSGVO gestützt werden.

Da diese Standarddatenschutzklauseln ihrer Natur nach keine Garantien bieten können, die über die vertragliche Verpflichtung, für die Einhaltung des unionsrechtlich verlangten Schutzniveaus zu sorgen, hinausgehen, kann es je nach der in einem bestimmten Drittland gegebenen Lage, erforderlich sein, dass der Verantwortliche zusätzliche Maßnahmen (siehe dazu Punkt II.3.6.2.2.2) ergreift, um die Einhaltung dieses Schutzniveaus zu gewährleisten.

II.3.6.2.2.2. Zu den zusätzlichen Maßnahmen:

In seinen „Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten, Version 2.0 des Europäischen Datenschutzausschusses („EDSA-Empfehlungen")" hat der EDSA festgehalten, dass für den Fall, dass das Recht des Drittlands sich auf die Wirksamkeit von geeigneten Garantien (wie etwa Standarddatenschutzklauseln) auswirkt, der Datenexporteur die Datenübermittlung entweder auszusetzen oder zusätzliche Maßnahmen zu implementieren hat (EDSA-Empfehlungen Rn 28 ff sowie Rn 52 bzw. EuGH 16.07.2020, C-311/18 *(Schrems II)*, Rn 121).

Solche „zusätzliche Maßnahmen" können laut den Empfehlungen des EDSA vertraglicher, technischer oder organisatorischer Art sein (EDSA-Empfehlungen, Rn 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"* (EDSA-Empfehlungen 01/2020, Rn 99).

Zu organisatorischen Maßnahmen wird ausgeführt, dass es sich *„[…] um interne Strategien, Organisationsmethoden und Standards handeln, die die Verantwortlichen und Auftragsverarbeiter bei sich selbst anwenden und den Datenimporteuren in Drittländern auferlegen könnten. Diese können zu einem im gesamten Verarbeitungszyklus einheitlichen Schutz personenbezogener Daten beitragen. Organisatorische Maßnahmen können auch dazu beitragen, dass sich die Datenexporteure der Risiken bezüglich des Datenzugriffs in*

Drittländern und entsprechender Zugriffsversuche besser bewusst sind und besser darauf reagieren können. 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 der Sache nach gleichwertigen Schutzniveaus) genügt. 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 der Sache nach gleichwertig ist" (EDSA-Empfehlungen 01/2020, Rn 128).

Zu den technischen Maßnahmen wird ausgeführt, dass diese *„[…] Garantien, die die Übermittlungsinstrumente in Art.l 46 DSGVO bieten, ergänzen können, um sicherzustellen, dass der unionsrechtlich erforderliche Schutz auch bei der Übermittlung personenbezogener Daten in ein Drittland gewährleistet ist. Diese Maßnahmen sind insbesondere dann erforderlich, wenn das Recht des betreffenden Drittlands dem Datenimporteur Verpflichtungen auferlegt, die den genannten Garantien der Übermittlungsinstrumente in Art. 46 DSGVO zuwiderlaufen und daher geeignet sind, die vertragliche Garantie eines der Sache nach gleichwertigen Schutzniveaus, was den behördlichen Datenzugriff im Drittland angeht, zu untergraben*" (EDSA-Empfehlungen 01/2020, Rn 77).

Eine zusätzliche Maßnahme ist nur dann als effektiv im Sinne des Urteils des Europäischen Gerichtshofes (EuGH 16.07.2020, C-311/18 *(Schrems II)*) anzusehen, sofern und soweit sie – für sich genommen oder in Verbindung mit anderen – genau die Rechtsschutzlücken schließt, die der Datenexporteur bei seiner Prüfung der für seine Übermittlung geltenden Rechtsvorschriften und Praktiken im Drittland festgestellt hat. Sollte es dem Datenexporteur letztendlich nicht möglich sein, ein der Sache nach gleichwertiges Schutzniveau zu erzielen, darf er die personenbezogenen Daten nicht übermitteln (EDSA-Empfehlungen 01/2020, Rn 75).

Umgelegt auf den gegenständlichen Fall bedeutet dies, dass zu untersuchen ist, ob die „zusätzlich getroffenen Maßnahmen" der BF2 (siehe Punkt II.1.10 bzw. VWA ./31, Seite 23 ff) die im Rahmen des Urteils des Europäischen Gerichtshofes (EuGH 16.07.2020, C-311/18 *(Schrems II)*) aufgezeigten Rechtsschutzlücken – also unangemessene Zugriffs- und Überwachungsmöglichkeiten von US-Nachrichtendienste sowie unzureichender wirksamer Rechtsbehelf für Betroffene – schließen.

Vor diesem Hintergrund ist daher zu prüfen, ob die von der BF2 zusätzlich getroffenen Maßnahmen geeignet sind, die rechtswidrigen Umstände – unverhältnismäßige

Zugriffsmöglichkeiten von US-Behörden bzw. der fehlenden wirksamen Rechtsbehelfe für Betroffene – zu beseitigen, damit die in Art. 7, 8 und 47 der Charta verbürgten Grundrechte nicht verletzt werden.

In Bezug auf die dargelegten vertraglichen und organisatorischen Maßnahmen ist nicht erkennbar, inwiefern durch eine Überprüfung einer Anfrage von US-Behörden durch XXXX -Anwälte bzw. durch speziell geschultes Personal, zwecks Einhaltung geltender Gesetze und XXXX -Richtlinien, die in Art. 7, 8 und 47 der Charta verbürgten Grundrechte nicht verletzt werden. Die Einhaltung von US-Gesetzen – also die Verpflichtung zur Herausgabe von Daten – führt gerade zur Verletzung der Grundrechte von betroffenen Unionsbürgern. Ebenso kommt der Benachrichtigung von Kunden kein Begründungswert zu, bevor eine ihrer Informationen US-Behörden bekannt gegeben wird. Dies deshalb, da eine Weitergabe von Informationen nach europäischem Recht unverhältnismäßig ist und der betroffene Unionsbürger keine wirksamen Rechtsbehelfe gegen eine Weitergabe hat. Auch kommt es zu einer Verletzung von Grundrechten von betroffenen Unionsbürgern, wenn eine Mitteilung an den Kunden aus US-gesetzlichen Gründen unterbleibt. Selbst wenn die Anfrage einer US-Behörde aufgrund eines Notfalles unterbleibt, ist die Weitergabe rechtswidrig, da der betroffene Unionsbürger nicht die Möglichkeit hat, mit Hilfe eines wirksamen Rechtsbehelfes den Notfall zu verifizieren. Schließlich können die Veröffentlichung eines Transparenzberichtes sowie die Veröffentlichung der Politik der BF2 im Umgang mit Regierungsanfragen die rechtswidrigen Umstände nicht beseitigen, damit die in Art. 7, 8 und 47 der Charta verbürgten Grundrechte nicht verletzt werden.

Auch die dargestellten technischen Maßnahmen sind nicht geeignet, um die Verletzung der Grundrechte zu beseitigen. So können die aufgezählten technischen Maßnahmen im Zusammenhang mit der Übertragung bzw. Speicherung der Daten die Zugriffsmöglichkeiten von US-Nachrichtendiensten auf Grundlage des US-Rechts weder verhindern noch einschränken. Wie zutreffend die bB ausführte, können die technischen Maßnahmen nicht als wirkungsvoll betrachtet werden, wenn die BF2 selbst nach wie vor die Möglichkeit hat, auf die Daten im Klartext zuzugreifen. Soweit die BF2 auf eine Verschlüsselungstechnologie hinweist, so ist aus EDSA-Empfehlungen zu entnehmen, dass ein Datenimporteur (die BF2), 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 (Rn 81).

Auch sind die Ausführungen der BF2, dass *soweit* XXXX *-Analytics Daten zur Messung durch Website-Besitzer personenbezogene Daten sind, als pseudonym betrachtet werden müssten*, nicht als „zusätzliche Maßnahme“ geeignet. In diesem Zusammenhang wird auf die überzeugende Ansicht der Deutschen Datenschutzkonferenz verwiesen, 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 der BF2 auch deshalb nicht zu folgen, weil die XXXX -Analytics Kennung ohnedies mit weiteren Elementen kombiniert und sogar mit einem dem BF2 unstrittig zuzurechnenden XXXX -Konto in Verbindung gebracht werden kann.

Die angesprochene „Anonymisierungsfunktion der IP-Adresse“ ist fallbezogen nicht von Relevanz, da diese nicht korrekt implementiert wurde (siehe Punkt II.1.3.4).

Insgesamt sind die von der BF2 aufgezeigten zusätzlichen Maßnahmen nicht geeignet, die im Urteil aufgezeigten Rechtsschutzlücken – unangemessene Zugriffs- und Überwachungsmöglichkeiten von US-Nachrichtendiensten sowie unzureichender wirksamer Rechtsbehelf für Betroffene – schließen.

II.3.6.2.2.3. Zusammenfassung:

Aufgrund der Entscheidung des Europäischen Gerichtshofes vom 16.07.2020, C-311/18 *(Schrems II)* war die verfahrensgegenständliche Datenübertragung nicht mit dem „EU-US Privacy Shield“ geschützt. Auch kann die verfahrensgegenständliche Datenübertragung nicht allein auf die zwischen der MB und der BF2 abgeschlossenen Standarddatenschutzklauseln gemäß Art. 46 Abs. 2 lit. c DSGVO gestützt werden. Darüber hinaus sind die von der BF2 aufgezeigten zusätzlichen Maßnahmen nicht geeignet, die im Urteil aufgezeigten Rechtsschutzlücken – unangemessene Zugriffs- und Überwachungsmöglichkeiten von US-Nachrichtendiensten sowie unzureichende wirksame Rechtsbehelfe für Betroffene – zu

schließen. Insgesamt findet die verfahrensgegenständliche Datenübermittlung keine Deckung in Art. 46 DSGVO.

Soweit die BF2 im verwaltungsbehördlichen Verfahren einen risikobasierten Ansatz unterstellt, ist zu beachten, dass sich dieser Ansatz schon mit dem Wortlaut des Art. 44 DSGVO nicht vereinbaren lässt. Art. 44 DSGVO erfasst jedwede Übermittlung von personenbezogenen Daten. Die Norm differenziert daher nicht danach, ob äußerst niederschwellige Daten übertragen werden für die ein nur sehr geringes Basisrisiko besteht. Zwar sieht die DSGVO in einzelnen Bestimmungen einen risikobasierten Ansatz vor (zB 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), jedoch führt dieser Umstand nicht dazu, dass der risikobasierte Ansatz analog auf Art. 44 DSGVO anzuwenden ist.

Der Europäische Gerichtshof (EuGH 16.07.2020, C-311/18 (*Schrems II*)) ist in Bezug auf die Rechtslage der USA nun gerade davon ausgegangen, dass aufgrund der unverhältnismäßigen Zugriffsmöglichkeiten von US-Behörden sowie unzureichender wirksamer Rechtsbehelfe für Betroffene gerade von keinem „angemessenen Datenschutzniveau“ auszugehen ist, weshalb er schließlich auch den EU-USA-Angemessenheitsbeschluss für ungültig erklärt hat. Der Europäische Gerichtshof hat ausdrücklich nicht darauf abgestellt, dass die Verpflichtungen, denen sich ein Privacy-Shield zertifiziertes Unternehmen aus den Vereinigten Staaten unterwirft, im Einzelfall möglicherweise doch angemessen sind (etwa, weil das zertifizierte Unternehmen bloß nicht-sensible oder nicht-strafrechtlich relevante personenbezogene Daten erhält).

Mit Hilfe der DSGVO soll auch der freie Datenverkehr gewährleistet werden. Jedoch steht der freie Datenverkehr in diesem Zusammenhang 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 jedoch nicht vorgesehen. Wirtschaftliche Interessen spielten auch im Urteil des EuGH vom 16.07.2020, C-311/18 (*Schrems II*) keine Rolle.

II.3.6.3. Zu den Ausnahmen für bestimmte Fälle gemäß Art. 49 DSGVO:

Entsprechend den eignen Angaben der MB war die Ausnahmeregelung gemäß Art. 49 DSGVO für die gegenständliche Datenübermittlung nicht von Relevanz (VWA ./11, Seite 13). Auch ist im Verfahren nicht hervorgekommen, dass eine Einwilligung gemäß Art. 49 Abs. 1 lit. a DSGVO eingeholt wurde. Da insgesamt keine Umstände hervorgekommen sind, dass ein Tatbestand gemäß Art. 49 DSGVO erfüllt wäre, kann die verfahrensgegenständliche Datenübertragung nicht auf Art. 49 DSGVO gestützt werden.

II.3.6.4. Ergebnis:

Da für die gegenständliche Datenübermittlung der MB an die BF2 (in den Vereinigten Staaten) kein angemessenes Schutzniveau durch ein Instrument von Kapitel V der DSGVO gewährleistet wurde, liegt eine Verletzung von Art. 44 vor. Die MB war (jedenfalls) zum beschwerderelevanten Zeitpunkt – also dem 14.08.2020 – für den Betrieb der Website XXXX verantwortlich. Der hier relevante datenschutzrechtliche Verstoß gegen Art. 44 DSGVO ist daher der MB zuzurechnen.

Insgesamt war die BF2 nicht in der Lage, eine Rechtswidrigkeit zu Spruchpunkt 2. der Entscheidung der bB zu begründen, welche ihre rechtlichen Interessen verletzt hätte. Auch aus diesem Grund war die Bescheidbeschwerde der BF2 abzulehnen.

II.3.7. Zu Spruchpunkt A.II) – Unzulässigkeit der Revision:

Gemäß § 25a Abs. 1 VwGG hat das Verwaltungsgericht im Spruch seines Erkenntnisses oder Beschlusses auszusprechen, ob die Revision gemäß Art. 133 Abs. 4 B-VG zulässig ist. Der Ausspruch ist kurz zu begründen.

Die Revision ist zuzulassen, weil es zur Frage, ob einem Datenempfänger (Datenimporteur in einem Drittstaat) im Verfahren über die Feststellung einer Verletzung der allgemeinen Grundsätze der Datenübermittlung gemäß Art. 44 DSGVO zukommt, noch keine hinreichende Judikatur des Verwaltungsgerichtshofes besteht.

Es war daher spruchgemäß zu entscheiden.

II.3.8. Zu Spruchpunkt B.I) – Abweisung der Bescheidbeschwerde des BF1:

Wie unter Punkt II.3.3 ausgeführt, sind aus Kapitel V DSGVO keine subjektiven öffentlichen Rechte/Pflichten die BF2 als Datenimporteur zu entnehmen. Vor diesem Hintergrund war die Bescheidbeschwerde des BF1 abzuweisen.

II.3.9. Zu Spruchpunkt B.II) – Zulässigkeit der Revision:

Gemäß § 25a Abs. 1 VwGG hat das Verwaltungsgericht im Spruch seines Erkenntnisses oder Beschlusses auszusprechen, ob die Revision gemäß Art. 133 Abs. 4 B-VG zulässig ist. Der Ausspruch ist kurz zu begründen.

Die Revision ist zuzulassen, weil zu der hier aufgezeigten Rechtsfrage noch keine hinreichende Judikatur des Verwaltungsgerichtshofes besteht.

Es war daher spruchgemäß zu entscheiden.