

GZ: D155.028
2022-0.726.643

Clerk: [REDACTED]

[REDACTED]
zH noyb - European Center for Digital Rights

Data protection complaint (Art. 77 para. 1 DSGVO, Section 24 para. 1 DSG)

[REDACTED] /1. [REDACTED], 2. Meta Platforms, Inc. (formerly Facebook Inc.)

[REDACTED]

CONTRIBUT
ION

The data protection authority decides on the data protection complaint of (com [REDACTED]
represented by NOYB - European Centre
for digital Rights, Goldschlagstraße 172/4/3/2, 1140 Vienna, ZVR:
1354838270, of 17 August 2022 against

1) [REDACTED] (first respondent), represented by [REDACTED]
[REDACTED] and 2) Meta Platforms, Inc. (second respondent), located at 1601 Willow
Rd, Menlo Park, CA, USA, for A) a violation of Article 44 of the GDPR by the respondents and B) a
violation of Article 5 et seq, Article 28 and Article 29 of the GDPR by the second respondent as
follows:

1. The decision of the data protection authority of 2 October 2020, ZI. D155.028, 2020-0.527.429, is repealed.
2. The complaint concerning grievance A) is partially upheld and it is stated that as a consequence of the decision of the first respondent as the data protection controller, the Facebook Business Tools "Facebook Login" and "Facebook Pixel" on the website [REDACTED], at least on 12 August 2020, personal data of the complainant (these are at least unique user identification numbers, IP address and browser parameters) were transferred to the second respondent in the USA (data transfer), although the

The first respondent has not ensured an adequate level of protection for this data transfer pursuant to Art. 44 GDPR.

3. Dismisses the complaint against the second respondent in respect of objections A) and B).

Legal basis: Art. 4 Z 1, Z 2, Z 7, Z 8 and Z 23 lit. b, Art. 5, Art. 28, Art. 29, Art. 44, Art. 46 Para. 1 and para. 2 lit. c, Art. 51 para. 1, Art. 57 para. 1 lit. d and lit. f, Art. 77 para. 1, Art. 80 para. 1 and Art. 93 para. 2 of Regulation (EU) 2016/679 (General Data Protection Regulation, GDPR), OJ No. L 119 of 4.5.2016 p. 1; Sections 18(1) and 24(1), (2)(5) and (5) of the Data Protection Act (Datenschutzgesetz, DSG), Federal Law Gazette I No. 165/1999 as amended; Section 68(2) of the General Administrative Procedure Act 1991 (Allgemeines Verwaltungsverfahrensgesetz, AVG), Federal Law Gazette 51/1991 as amended.

C O N S I D U C A T I O N

A. Arguments of the parties and course of proceedings

A.1. In his submission of 18 August 2020, the complainant submitted the following in summary:

On 12 August 2020, the complainant had visited the first respondent's website at while in the [REDACTED] Facebook account linked to the email address [REDACTED] had been logged in. The first respondent had embedded the HTML code for Facebook services (including Facebook Connect) on its website. In the course of the visit to the website, personal data of the complainant (at least the IP address and cookie data) had been transmitted to the second respondent. The transmission of the complainant's data had been unlawful. It was requested to investigate whether the requirements of Art. 28 GDPR were met with regard to the transfer of data to the USA and to impose a ban or suspension of any data transfers from the first respondent to the USA and to order a return of these data to the EU.

The submission was accompanied by a bundle of documents.

A.2. By decision of 2 October 2020, ZI. D155.028, 2020-0.527.429, the data protection authority suspended the complaint procedure in question.

A.3. With Statement [REDACTED] from 28. December 2020 brought the respondent submitted the following in summary:

The website [REDACTED] the online presence of the daily [REDACTED] newspaper [REDACTED]. A

Data processing in connection with a Facebook tool had taken place exclusively for journalistic purposes, and the media privilege standardised in section 9(1) of the Data Protection Act applied. Without prejudice to the factual and legal situation, the first respondent had taken all Facebook tools on the website [REDACTED] offline or deactivated 19 November 2020.

A bundle of documents was attached to the statement.

A.4. In his statement of 22 January 2021, the complainant submitted the following in summary:

The data processing in connection with the Facebook tools was not for journalistic purposes. The complainant had also not interacted during the visit in a way that could have been for journalistic purposes. He had visited the website [REDACTED] merely visited. In the event that the data protection authority assumes that the infringement will be remedied retroactively pursuant to Section 24 (6) of the Data Protection Act, a declaration is requested that the first respondent has unlawfully transferred personal data to the USA.

A bundle of documents was attached to the statement.

A.5. The data protection authority requested the respondent to the second complaint to answer several questions in connection with the Facebook tools in its reply of 26 February 2021. In a letter dated 18 March 2021, the second respondent stated that Facebook Ireland Limited was competent to deal with the data processing in question. Subsequently, the Irish supervisory authority was requested by the data protection authority under the cooperation mechanism pursuant to Article 57(1)(g) of the GDPR to forward questions relating to the Facebook Connect tool to Facebook Ireland Limited. Subsequently, the Irish supervisory authority forwarded the answered questionnaire from Facebook Ireland Limited, dated 5 May 2021, to the data protection authority.

A.6. In his observations of 10 May 2021, the complainant submitted the following in summary:

The present complaint is explicitly directed against the first and second respondents and Facebook Ireland Limited (note by the data protection authority: The complaint against Facebook Ireland Limited was later withdrawn, see below). The data protection authority had jurisdiction over the second respondent in its role as data importer.

A.7. After several requests by the data protection authority, the second respondent submitted the following in summary in its statement of 22 June 2021

The second respondent was a sub-processor and the scope of the GDPR did not apply. The data processing subject of the complaint was not carried out by the second respondent, which was the sole recipient of the data. The main office is located in Ireland and the contact person is Facebook Ireland Limited.

A.8. The data protection authority issued a second mutual assistance request to the Irish supervisory authority (DPC) responsible for Facebook Ireland Ltd on 18 August 2021. The subject of the request for assistance was data processing in connection with Facebook tools. (Note by the data protection authority: The questionnaire was sent to Facebook Ireland Limited by the Irish supervisory authority on 31 January 2022. On 7 February 2022, Facebook Ireland Limited sent a general response without specifically addressing the questions contained in the list of questions. The list of questions was no longer relevant from the perspective of the data protection authority, since, as can be seen below, an oral hearing was subsequently scheduled).

A.9. In his observations of 24 September 2021, the complainant submitted the following in summary:

The complaint against Facebook Ireland Limited was withdrawn, while the complaint against the first and second respondents was maintained. Chapter V of the GDPR does not differentiate between controllers and processors. The question of the allocation of roles therefore appears to be only a preliminary question regarding the competence of the data protection authority. The distribution of roles was such that the first respondent was to be qualified as a controller and the second respondent at least as a (sub)processor receiving the data in the USA. Due to the Facebook services and the group structure of the Facebook group, it was obvious that there was joint responsibility between the second respondent and Facebook Ireland Limited. Facebook Ireland Limited was also not a branch of Facebook Inc. The data protection authority was asked to review the procedural file on no. IN-20-8-1 (note on data protection). IN-20-8-1 (note by the data protection authority: this is a procedure before the Irish supervisory authority) within the framework of administrative assistance pursuant to Art. 61 GDPR. Chapter V of the GDPR is also relevant for data recipients in the third country, as a transfer without a recipient is not possible. In the event that the data protection authority does not consider itself competent to deal with the complaint against the second respondent, a decision on competence in the form of a decision is requested.

A.10. The data protection authority scheduled an oral hearing with the second respondent. In addition, the data protection authority sent a list of questions to the first respondent on 5 January 2022.

A.11. In its statement of 7 March 2022, the first respondent submitted the following in summary:

At the time of the complaint, the first respondent had used the Facebook Pixel Tracker on its website [REDACTED] in addition to Facebook Connect (or Facebook Login).

integrated. The Facebook Pixel Tracker was expanded on 7 December 2020. The use of Facebook Login served to provide premium customers with a simplified login option. Facebook Login was subsequently expanded in January 2022. The first respondent had issued an instruction or notification to Facebook Ireland Limited that it should transfer the processed data for law enforcement purposes and then delete it. With the integration of Facebook Login, personal data of the public profile of the respective logged-in user was transferred to the first respondent. As of 7 March 2022, the respondent no longer used Facebook Business Tools.

A.12. The oral hearing of the second respondent was held on 16 May 2022 (note by the data protection authority: by video conference pursuant to section 51a AVG). The corrected version of the transcript ("Transcript of the oral hearing of Meta Platforms Inc Final.pdf") is attached to the file.

A.13. On 30 May 2022, the second respondent submitted a document ("data list"), to which in the context of the oral hearing of 16 May 2022.

A.14. In his observations of 25 July 2022, the complainant submitted the following in summary:

complainant had not actively interacted with Facebook Login when visiting [REDACTED]. Immediately after opening the website or interacting with the cookie banner, the data transfers visible in the HAR file occurred. Due to the host designation "connect.facebook.net", he had assumed the use of "Facebook Connect". It was not possible to determine which specific Facebook tools had triggered the data transfers. The complaint generally referred to the transfer of the complainant's personal data to Facebook Connect.

The second respondent was arrested [REDACTED] on the occasion of the visit of 12 August 2020.

The complainant requested a declaration of a violation of Article 44 of the GDPR, as the data transfer on 12 August 2020 was not justified by any transfer mechanism pursuant to Article 45 et seq. of the GDPR. Furthermore, he requested a declaration of a violation of Art. 28 in conjunction with Art. 5 et seq. in conjunction with Art. 29 GDPR as a result of the aforementioned violation of Art. 44 GDPR. The infringements were in the past and had been completed. Whether the Facebook tools that triggered the data transfer to the USA on 12 August 2020 have been removed in the meantime is [REDACTED] irrelevant for the complaint proceedings. The application for the imposition of a fine is withdrawn.

A.15. In its statement of 19 September 2022 [REDACTED] the second respondent submitted the following in summary:

The second respondent was a (sub-)processor and merely a recipient of the data subject of the complaint. In this context, the data processing was not subject to the territorial scope of the GDPR. With regard to the role of Meta Ireland, this is best discussed with Meta Ireland. Reference is made to the [website https://m.facebook.com/legal/businessstech](https://m.facebook.com/legal/businessstech). Meta Ireland is the data exporter. The data transfers in question were lawful and in accordance with Chapter V of the GDPR. The subject of the complaint was the Facebook Login tool; the complaint could not "generally" be about the transfer of data to the USA.

A.16. In his observations of 18 October 2022, the complainant submitted the following in summary:

The subject matter of the complaint was the data transfers on 12 August 2020. The facts of the case were unambiguously described by means of the URL visible to the complainant in the code and in the traffic, various product names were irrelevant. The complaint related to the transfer of personal data to the USA.

A.17. With Statement from 18. October 2022 brought the respondent submitted the following in summary:

Facebook Ireland Limited had acted as the primary contractual partner. The data processing that took place in 2020 could no longer be clearly traced by the first respondent without the possibility of access. The processed data and the logs in connection with the Facebook pixel tracker were no longer within its sphere of influence. The accused infringement had been completely eliminated. In the case at hand, no violation of section 1 of the DPA was the subject of the complaint; the facts of the case were different. Therefore, section 24(6) of the FADP was relevant. It was requested that the proceedings in this case be suspended until the preliminary ruling by the ECJ in Case No. C-446/21. An annex entitled "Confidential" was attached to the minutes of the oral hearing of the second respondent on 16 May 2022. This letter had not been served on the first respondent.

B. Subject of the complaint

B.1. Establishment of an infringement which lies in the past

a) On the request for determination

Art. 58 GDPR does not contain an explicit legal basis for an independent determination of the possible unlawfulness of a processing operation relevant under data protection law (cf. Administrative Court of 1 September 2022, Ra 2022/04/0066). Accordingly, the mere determination of an

In the event of an infringement of a right protected by data protection law pursuant to Article 58(6) of the GDPR in conjunction with Section 24(2)(5) of the GDPR, a request by the data subject is required.

In his first submission of 17 August 2020, the complainant did not make an explicit request within the meaning of Section 24(2)(5) of the DPA. Rather, the requests (see below) were directed at an infringement that was still ongoing (at the time of the submission).

In the course of the proceedings, the complainant made it clear that, in the context of his complaint, a violation of the law may be established as of 12 August 2020:

While the complainant still requested this finding with certain reservations in its opinion of 22 January 2021 ("*... in the event that the DPA assumes that the infringement will be subsequently remedied pursuant to Section 24 (6) DPA, the respondent requests that the*

Find that the respondent improperly collected personal data on 12.08.2020.

data of the complainant to the USA [...]", the complainant clarifies in its statement of 24 September 2021 and in particular of 25 July 2022 that the date of the complaint is 12 August 2020 and that the infringement is not amenable to a remedy within the meaning of Section 24 (6) DPA. These statements were also brought to the attention of the respondents.

From the perspective of the data protection authority, there is therefore a clear reference to Section 24 (2) (5) of the Data Protection Act in the present case and the complainant's intention is recognisable that the determination of a past violation of the law should be adjudicated.

b) On the infringements

It is clear from the complainant's submission of 17 August 2020 and, in particular, his statement of 25 July 2022 that the subject matter of the complaint is, in general, data transfers on 12 August 2020 to the US related to Facebook Business Tools ("*... On the website, the controller has embedded the HTML code for Facebook services [including Facebook Connect]*"). The complainant also did not at any time limit his complaint to data processing that took place only as a result of the implementation of Facebook Login.

Taking into account this consideration as well as the complainant's further statements of 22 January 2021 and 24 September 2021, the following legal violations are to be decided upon:

Objection A): Did the Respondents, due to the implementation of Facebook Business Tools on the Website, at  least on 12 August 2020

personal data of the complainant transferred to the USA without ensuring an adequate level of protection pursuant to Art. 44 GDPR?

Objection B): Did the second respondent, in the course of the contested data transmission on 12 August 2020 violate Art. 5 et seq. in conjunction with Art. 28 in conjunction with Art. 29 GDPR?

B.2. On the processing ban

It is not necessary to rule on the complainant's request for an immediate ban on any data transfers pursuant to Article 58(2)(d), (f) and (j) of the GDPR, as the first respondent removed the Facebook Business Tools from its website before the conclusion of the present proceedings.

B.3. On the application for the imposition of a fine

There is no need to rule on the complainant's request to impose a fine on the respondents, as this request was withdrawn in the opinion of 25 July 2022 (and is now to be understood as a suggestion).

C. Findings of fact

C.1. On the general functioning of cookies

Cookies can be used to collect information generated by a website and stored via an internet user's browser. It is a small file or text information (usually smaller than one Kbyte) that is placed by a website on the hard drive of an internet user's computer or mobile device via their browser.

A cookie allows the website to "remember" the user's actions or preferences. Most web browsers support cookies, but users can set their browsers to reject cookies. They can also delete the cookies at any time.

Websites use cookies to identify users, remember their customers' preferences and allow users to complete tasks without having to re-enter information when they move to another page or revisit the website later.

Cookies can also be used to collect information for targeted advertising and marketing based on online behaviour. For example, companies use software to track user behaviour and create personal profiles that allow them to show users ads tailored to their previous searches.

Evaluation of evidence C.1.: The comments on the functioning of cookies are taken from the Advocate General's Opinion in Case C-673/17, paragraph 36 et seqq. Since it is a

As the description of the possible functions of cookies is independent of the individual case and is of a general technical nature, these explanations were to be included at the level of the facts - and not in the legal assessment.

C.2. On the general functioning of Facebook Login

Facebook Login is a tool offered by the Meta Group. Facebook Login can be integrated into web services or apps that are not offered by the Meta Group. This allows users to log in to third-party web services or apps with their Facebook user data without having to register separately.

Facebook Login was offered a long time ago under the name Facebook Connect.

The Meta Group provides the following information on Facebook Login at <https://developers.facebook.com/docs/facebook-login/overview> (excerpt, formatting not reproduced 1:1, links not included):

" Facebook Login - Overview

Facebook Login allows users to securely and easily create accounts and log in to your app across multiple platforms. This feature is available for iOS, Android, web, desktop apps and devices such as smart TVs and Internet of Things objects. Facebook Login allows you to access personal data via authentication or permission request. You can use Facebook Login for authentication only or additionally for data access.

[...]

Use cases

Facebook Login enables a great user experience in a number of ways:

- **Account creation**

With Facebook Login, users can quickly and easily create an account for your app and do not need a password that they can easily forget. This leads to higher conversion. Once a user has created an account on one platform, they can log in to your app on all other platforms - often with a single click. A validated email address allows you to reach and interact with the user at a later time.

- **Personalisation**

A personalised user experience connects the user more with your app and leads to higher user retention. Facebook Login allows you to collect information that you would normally have to collect in a complicated and tedious way through your own registration form. Even if a user can only import a profile picture from Facebook into your app, they already feel more connected to your app.

[...]

Functions

- **True identity**

When a user chooses to log in through Facebook, he/she does so with his/her true identity. The public profile includes a person's real name and a profile picture. Apps that rely on true identities tend to get less spam and encourage higher quality conversations.

- **Cross-platform login**

Facebook Login is available on the most popular mobile and desktop app platforms. Users who create accounts on one platform through Facebook can also quickly and easily log in to your app on another platform. A person always has the same user ID wherever they are, ensuring a seamless cross-platform app experience. Facebook Login is available for iOS, Android and web, for desktop apps and for devices such as smart TVs and Internet-of-Things devices.

- **Works together with your existing account system**

Facebook Login complements your existing account system. Give your users the option of logging in via Facebook in addition to email, SMS or other social networks. If an email address received through Facebook Login matches an email address that already exists in your system, that user can log in to their existing account without entering a password.

- **Precise authorisations**

Facebook Login supports many permissions that determine what information users share with your app. For you, this means that you have complete control over what permissions you request, and users have control over how they allow the app to use their data.

- **People have control over what they share**

A great user experience requires users to have control over what they do and don't want to share. With Facebook Login, users can specify exactly what information they want to share with your app. Even if they don't want to share certain information with you because they feel uncomfortable, they still get the benefits of Facebook Login. Your app can request this information again at a later time after you have explained to users how you will use their information to provide them with a better user experience.

- **Step-by-step authorisation**

Facebook Login supports step-by-step authorisation. This means that you don't have to request all the required information immediately, but can do so gradually. This makes it quick and easy for users to create an account for your app. Once they are more familiar with your app, you can request more permissions to improve their user experience.

- **Express login**

Express Login logs people in to their Facebook account on all devices and platforms. If a person has previously signed in to your app on any platform, you can use Express Login to sign them in to their Facebook account on Android. This doesn't require the person to select a login method, which could lead to duplicate accounts being created or people not logging in at all."

Evaluation of evidence C.2.: The findings made regarding the functioning of Facebook Login are based on on a official research of the website <https://developers.facebook.com/docs/facebook-login/overview> (retrieved on 6 March 2023).

The finding that Facebook Login was offered under the name Facebook Connect a long time ago is based on the testimony of the second respondent during the oral hearing on 16 May 2022 (answer to question 8).

C.3. On the general functioning of Facebook Pixel

The Meta Group provides the following information on Facebook Pixel (now: Meta Pixel) at <https://developers.facebook.com/docs/meta-pixel/> (excerpt, formatting not reproduced 1:1, links not included):

"Meta Pixel

The meta pixel is a JavaScript code snippet that allows you to track the activity of visitors to your website. It works by loading a small library of functions that you can use whenever a site visitor takes an action (called an event) that you want to track (this action is called a conversion). Tracked conversions appear in the dashboard of the ad manager. They can be used there to measure the effectiveness of your ads, set Custom Audiences for ad targeting, Advantage+ Catalog Ads campaigns, and analyse the effectiveness of your website's conversion funnels.

The meta pixel can collect the following data:

- **HTTP header** - all information contained in HTTP headers. HTTP headers are a standard web protocol that is sent between all browser requests and all servers on the Internet. The HTTP headers include IP addresses, information about the web browser, the location of the page, the document, the referrer and the person using the web page.
- **Pixel-specific data** - including the pixel ID and the Facebook cookie.
- **Button click data** - all buttons clicked by visitors to the website, the labels of those buttons and all pages accessed as a result of those button clicks.
- **Optional values** - Developers and marketers can optionally set custom data events to send additional information about the visit. Examples of custom data events include conversion value and page type.
- **Form field names** - Including website field names such as email, address, quantity, for the purchase of a product or service. We do not collect field values unless they are part of Advanced Matching or optional values."

The Meta Group also provides the following information on Meta Pixel at <https://de-de.facebook.com/business/help/742478679120153?id=1205376682832142> (excerpt, formatting not reproduced 1:1, links not included):

"Use the meta pixel for the following purposes:

- *Deliver your ads to the right people. Find new customers or people who have visited a specific area of your website or taken a desired action.*
- *Increase your sales. Set up automated bids to reach people who are more likely to take an action that is relevant to you, such as making a purchase.*
- *Measure the success of your ads. Analyse the impact of your ads by capturing user reactions.*

After you set up your meta pixel, it logs when someone takes an action on your website. Such actions are, for example, adding an item to the shopping cart or completing a purchase. The meta pixel records these actions (also called events), which you can then view in the Events Manager on your meta pixel's page. Here you can see the actions that your customers take. You can also retarget these customers with further Facebook ads.

If you share events with Meta via the Pixel, we recommend that you also use the Conversions API. In combination with your pixel, the Conversions API helps you to improve the performance and measurement of your Facebook advertising campaigns. Here you can find more information about the Conversions API.

The terms of use for our business tools state that businesses (or partners acting on their behalf) may not install a pixel linked to their Business Manager or advertising account on websites they do not own without our written permission. From 5 May 2021, we will show verified domain owners the events and custom conversions we have recently received via the meta pixels placed on their websites. While verified domain owners will be able to see all events, they will only be able to use events for ad optimisation and reporting if they can also access these events in their own Business Manager account. If you don't want information from your meta pixel or custom conversions to be visible to the domain owner, you can remove the pixel from the site or delete the custom conversion by the date specified."

Meta Ireland processes the data of Austrian users who use Facebook Business Tools and the second respondent receives instructions from Meta Ireland in this regard.

Evaluation of evidence C.3.: *The findings on the functioning of Facebook and Meta Pixel are based on an official search of the website <https://de-de.facebook.com/business/help/742478679120153?id=1205376682832142> as well as <https://developers.facebook.com/docs/meta-pixel/> (both retrieved on 6 March 2023).*

The finding that the second respondent receives all instructions related to Facebook Business Tools from Meta Ireland is based on the credible testimony of the second respondent during the oral hearing on 16 May 2022 (answer to question 2). Although the second respondent only referred to Facebook Login in her testimony, there is no factual reason to assume that these considerations do not apply to Facebook Business Tools in general. Nor can anything to the contrary be deduced from the terms of use and data processing conditions for Facebook Business Tools (which include Facebook Login and Facebook Pixel), which can be seen below.

C.4. About the Cookie Policy of Meta Platforms Ireland Limited (previously: Facebook Ireland Limited)

Meta Platforms Ireland Limited provides the following information on cookies at <https://www.facebook.com/policies/cookies/> (extract, formatting not reproduced 1:1, links not included):

"Where do we use cookies?"

We may place cookies on your computer or device to obtain information that is stored in the cookies when you use or visit the following:

- The meta-products;
- Products provided by other members of the Meta Companies; and
- Websites and apps provided by other companies that use Meta products, including companies that embed Meta technologies into their websites and apps. Meta uses cookies and receives information when you visit such websites and apps, including device information and information about your activity, without any further action on your part. This happens regardless of whether you have a Facebook account or are logged in."

Evaluation of evidence C.4.: The findings made are based on an official search of the website

<https://www.facebook.com/policies/cookies/> (retrieved on 6 March 2023).

C.5. To the Terms of Use for Facebook Business Tools

The terms of use for Facebook Business Tools (as of 26 December 2019) were as follows on 12 August 2020 as follows (formatting not reproduced 1:1, links not included):

"These terms of use will be updated with effect from 31 August 2020. To give you a To preview the new version before it comes into effect, click here.

Terms of Use for Facebook Business Tools

Facebook Business Tools are a subset of Facebook products. We provide these tools to help website owners and publishers, developers, advertisers, business partners (and their customers), and others integrate and use information and share it with Facebook. Facebook Business Tools include the following: APIs and SDKs, the Facebook Pixel, social plugins such as the "Like" and "Share" buttons, Facebook Login and Account Kit and other platform integrations, plugins, codes, specifications, documentation, technologies and services. By clicking "Agree" or using any Facebook business tool, you agree to the following:

1. Sharing personal data with Facebook

a. You may use Facebook Business Tools to send us personal information about your customers and users ("**Customer Data**"). Depending on which Facebook products you use, Customer Data may include the following:

i. "**Contact information**" consists of information that personally identifies data subjects, such as names, email addresses and telephone numbers. We only use this for matching purposes. We hash the contact information that you send us via a Facebook JavaScript pixel for matching purposes before submitting it. If you or your service provider uses a Facebook Image Pixel or other Facebook Business Tools, you or your service provider must hash the contact information in a manner specified by us prior to submission.

ii. "**Event Data**" includes other information you share about your customers and the actions they take on your websites and in your apps or shops, such as visits to your websites, installations of your apps, and purchases of your products.

b. Customer data does not include information where a data subject specifically instructs you to share that information on our platform, such as an article shared via social plugins or other integration or a song so shared.

c. Subject to paragraph 1(d), we will not share the Customer Data you provide to us with any third party (including advertisers) unless we have your permission or are required by law to do so. We maintain the confidentiality and security of Customer Data by, among other things, appropriate organisational, technical and physical safeguards designed to (a) protect the security and integrity of Customer Data while it is on our systems and (b) protect Customer Data against accidental or unauthorised access, use, modification or disclosure within our systems.

d. You agree that Facebook may provide a specific individual with access to and/or a copy of their Event Data upon their request.

e. You represent and warrant that you have (and that any data provider you may use has) a legal basis (subject to all applicable laws, regulations and industry policies) for disclosing and using the Customer Data. If you did not collect the Customer Data directly from the data subject, you represent and warrant, without limiting any part of these Business Tools Terms of Use, that you have all necessary rights and permissions and a legal basis to disclose and use the Customer Data.

f. You will promptly notify us in writing of any actual or threatened complaint or challenge related to the use of personal information under these Business Tools Terms of Use and cooperate with us in responding to any such complaint or challenge.

g. If you are using the Client Data on behalf of a third party, you further represent and warrant that you are authorised as such third party's agent to use and process such data on its behalf and to bind such third party to these Business Tools Terms of Use. You will only use the Customer Data or any audience or report generated by your use of the Customer Data on behalf of such third party.

h. You will not share any customer information with us that you know or reasonably should know is from or about children under the age of 13 or that contains health, financial or other categories of confidential information (including any information that is considered confidential under applicable law).

2. Use of customer data

a. Depending on which Facebook company products you use, we use customer data for the following purposes:

i. Contact information for matching

1. You authorise us to process the contact information solely for the purpose of matching it with Facebook or Instagram user IDs ("**Matched User IDs**") and combining those user IDs with corresponding event data. We delete contact information after the matching process.

ii. Event data for measurement solutions and analysis services

1. You authorise us to process Event Data for the following purposes: (a) to produce reports on your behalf about the impact of your advertising campaigns and other online content ("**Campaign Reports**"); and (b) to produce analytics and insights about your customers and their use of your apps, websites, products and services ("**Analytics**").

2. We grant you a non-exclusive and non-transferable licence to use the campaign reports and analytics solely for your internal business purposes or in aggregated and anonymised form for measurement purposes only. You may not, without our written consent

Not disclose campaign reports or analytics, or any part thereof, to any third party. We will not disclose the campaign reports or analytics, or any part thereof, to any third party without your permission unless (i) they have been combined with campaign reports and analytics from numerous other third parties and (ii) your personal information is removed from the combined campaign reports and analytics.

iii. Event data for the creation of responsive target groups

1. We may process Event Data to create audiences (including Custom Audiences via websites, Custom Audiences via mobile apps and offline Custom Audiences) based on shared Event Data, which you may then use to target advertising campaigns. At our sole discretion, we may also allow you to share these audiences with other advertisers.

ii. Event data for the delivery of commercial and transactional messages

1. We may use the matched user IDs and associated event data to help you reach people with transactional and other commercial messages in Messenger and other Facebook company products.

ii. Event data to personalise features and content and to improve and secure Facebook products

1. We use event data to personalise the features and content (including ads and recommendations) we show to people on and off our Facebook Companies products. In connection with ad targeting and optimising ad delivery, we do the following: (i) we only use your Event Data to optimise delivery after aggregating it with other data collected by other advertisers or otherwise on Facebook Products; and (ii) we do not allow other advertisers or third parties to target ads based solely on your Event Data.

2. We may also use Event Data to promote safety and security on and off Facebook Companies' products and for research and development purposes and to maintain the integrity of and improve Facebook Companies' products.

2. Special provisions for the use of the Facebook Pixel and SDKs

a. You may not (or affiliates acting on your behalf may not) place pixels associated with your Business Manager or Advertising Account on websites that you do not own without our written permission.

b. If you use our pixels or SDKs, you also warrant and represent that you have provided a robust and prominent notice to users regarding the collection, sharing and use of customer data, which must include at least the following information:

i. For websites: A clear and conspicuous notice on each page of the website where our pixels are used. Such notice shall link to a clear explanation of (a) how third parties, including Facebook, may use cookies, web beacons and other storage technologies to collect or obtain information from your websites and other places on the Internet and then use that information to provide measurement services and ad targeting, (b) how users can opt-out of the collection and use of information for ad targeting, and (c) where users can access a mechanism to make such choices (e.g., by providing links to and). e.g. by providing links to <http://www.aboutads.info/choices> and <http://www.youronlinechoices.eu/>).

ii. For apps: A clear and prominent link that is easily accessible in your app settings or in any data policy and from any store or website where your app is distributed. This link must link to a clear explanation of (a) how third parties, including Facebook, may collect or receive information from your app and other apps and then use that information to provide measurement services and ad targeting, and (b) how and where users can opt out of the collection and use of information for ad targeting.

c. In jurisdictions where informed consent is required to store and access cookies or other information on an end user's device (such as the European Union), you must verifiably ensure that an end user provides the required consent before using Facebook Business Tools to allow us to store and access cookies or other information on the end user's device. (For suggestions on how to implement consent mechanisms, please see Facebook's Cookie Consent Guide for Sites and Apps).

3. Amendment, termination and storage:

a. We may change, suspend or terminate your access to, or the availability of, Facebook Business Tools at any time. You may terminate your use of Facebook Business Tools at any time. Subject to these Business Tools Terms of Use, we may store Event Data for a maximum of two years. We will store any audiences you create using the Event Data until you delete them from your account tools.

b. These Business Tools Terms of Use govern your provision of customer information to us and your use of Facebook Business Tools. Your use of these Facebook Business Tools may also be subject to Facebook Platform Policies. These Business Tools Terms of Use do not supersede any terms of use that apply to your purchase of advertising inventory from us (such as, but not limited to, the Facebook Advertising Guidelines at <https://www.facebook.com/policies/ads>). Such terms of use will continue to apply to your advertising campaigns. Facebook's Custom Audiences Terms of Use (currently available at <https://www.facebook.com/ads/manage/customaudiences/tos>) do not apply to audiences created through the processing of event data under these Business Tools Terms of Use. We reserve the right to monitor or review your compliance with these Terms of Use for Business Tools.

c. Hint:

i. We have updated the Terms of Use for Conversion Tracking, for Custom Audiences through your website, and for Custom Audiences through your mobile app, including changing their name to the Terms of Use for Facebook Business Tools. For purposes of the Facebook Business Tools Terms of Use, references in existing Terms of Use or agreements to "Facebook Tools" now mean Facebook Business Tools.

ii. We have updated our Terms of Use for Offline Conversions, including changing their name. They are now called the Facebook Business Tools Terms of Use. For purposes of the Facebook Business Tools Terms of Use, the following applies to references in existing terms of use or agreements: (i) "Sales Data" is now Customer Data, (ii)

"User Information" is now called Contact Information, (iii) "Sales Transaction Data" is now Event Data, (iv) "Matched Data" is now Event Data that has been combined with matched User IDs, (v) "Unmatched Data" is now Event Data that has not been combined with matched User IDs, (vi) "Reports" is now called Campaign Reports and (vii)

"OC" now stands for our offline conversion function.

d. As with our Commercial Terms, we may make changes to these Supplemental Terms of Use. If, after any update to the Additional Terms of Use, you continue to access any Facebook products that are subject to the Additional Terms of Use, you will not be able to use them.

Terms of Use, you agree to be bound by them. The parties acknowledge and agree that the State Specific Terms of Use apply to the provision and use of Facebook Business Tools and are incorporated by reference into these Business Tools Terms of Use.

e. Nothing in these Business Tools Terms of Use prevents us from making disclosures to our users in connection with Facebook Business Tools that we may be directed to make or that we may deem appropriate or required by applicable law.

4. A note for data controllers in the EU and Switzerland:

a. To the extent that the Customer Data includes personal data that you process pursuant to the General Data Protection Regulation (Regulation (EU) 2016/679) (the "GDPR"), the parties acknowledge and agree that you are the data controller with respect to such personal data for the purposes described in paragraphs 2.a.i and 2.a.ii above for the purposes of providing matching, measurement and analytics services, you are the data controller in respect of such Personal Data and that you have appointed Facebook Ireland Limited to process such Personal Data on your behalf as your processor in accordance with these Terms of Use and Facebook's Data Processing Terms, which are incorporated by reference into this document. "Personal Data", "Data Controller" and "Processor" in this paragraph shall have the meanings ascribed to them in the Data Processing Conditions.

Date of entry into force: 26 December 2019".

The Terms of Use for Facebook Business Tools were updated on 31 August 2020. The Terms of Use as amended on 31 August 2020 contain a reference to a new Data Transfer Addendum that incorporated standard contractual clauses into the contractual framework and replaced Privacy Shield. This addendum also entered into force on 31 August 2020:



The Terms of Use for Facebook Business Tools as amended on 26 December 2019 and the Terms of Use for Facebook Business Tools as amended on 31 August 2020 shall form the basis for the findings of fact.

Evaluation of evidence C.5: The findings made are based on the complainant's submission of 17 August 2020 and the documents submitted therein (Exhibit .I01 and Exhibit .I03). The stated terms of use for Facebook Business Tools as amended on 26 December 2019 and 31 August 2020 are contained in the file in question and are known to the parties. Furthermore, the findings are based on an official search of the website <https://m.facebook.com/legal/terms/businessstools> (retrieved on 6 March 2023).

C.6. To the data processing conditions for Facebook Business Tools

The data processing terms and conditions for Facebook Business Tools were as follows on 12 August 2020 (formatting not reproduced 1:1, links not included):

"These Terms of Use will be updated with effect from 31 August 2020. To give you a To preview the new version before it comes into effect, click here.

Data processing conditions

If you reside in the European Union or Switzerland, you acknowledge that your use of certain Facebook Products may involve the transfer of Personal Data (as defined below) to Facebook. To the extent that we process such data as your Processor (as defined below), these Terms of Use for Data Processing apply in addition to the applicable Product Terms of Use, such as the Facebook Business Tools Terms of Use and Custom Audiences Terms of Use ("Applicable Product Terms of Use"). In the event of a conflict with the Applicable Terms of Use, these Processing Terms will prevail.

Facebook and you agree on the following:

1. Data processing conditions

1. Facebook has

1. process personal data only in accordance with the applicable product terms of use;

2. take appropriate technical and organisational measures to protect personal data;

3. assist you, where possible (taking into account the nature of the processing), with appropriate technical and organisational measures to comply with your obligation to respond to requests to exercise data subject rights under the GDPR;

4. assist you in complying with your obligations under Articles 32 to 36 of the GDPR, taking into account the nature of the processing and the information available to Facebook;

5. upon termination of the applicable Product Terms, delete the personal data as soon as reasonably possible and within a maximum period of 180 days, unless EU law or the law of the EU Member State requires longer retention, in which case Facebook may retain the personal data longer if necessary to provide other services set forth in the applicable Product Terms;

6. Provide you with all information necessary to demonstrate Facebook's compliance with its obligations as a processor set out in Article 28 of the GDPR; and

7. arrange for an external auditor to conduct an annual SOC 2 Type II audit of the Data Processing Services as part of Facebook's audit programmes, or such other industry standard audit as Facebook may deem appropriate. Upon your request, Facebook will provide you with a copy of its most recent audit report no more than once per year, which will be considered Facebook's confidential information.

2. You agree that Facebook may subcontract its data processing obligations under these Terms of Use to a Data Processor

may. However, this can only be done through a written agreement with the sub-processor that imposes obligations on the sub-processor that are no less onerous than those imposed on Facebook by these Terms of Use for Data Processing. If a sub-processor fails to comply with such obligations, Facebook shall remain fully liable to you for the performance of such sub-processor's obligations. You hereby authorise Facebook to engage Facebook Inc. (and other Facebook companies) as its sub-processor(s). Facebook shall notify you in advance of (any) additional sub-processor(s). If you reasonably object to any such additional sub-processor(s), you may notify Facebook in writing of the reasons for your objection. If you object to any such additional sub-processor(s), you should stop using the Services and providing data to Facebook.

3. If Facebook becomes aware of any actual or suspected personal data breach involving personal data, Facebook shall promptly notify you. Such notification shall include the following information either at the time of notification or as soon as practicable thereafter: Details of the nature of the breach, the number of records affected, the category and approximate number of individuals affected, the likely consequences of the breach, and any actual or proposed measures to mitigate the possible adverse effects of the breach.

4. Facebook, Inc. has made commitments under the EU-U.S. Privacy Shield and the Swiss-U.S. Privacy Shield that may apply to data that has been/will be transferred to Facebook, Inc. by you or Facebook Ireland Limited under the applicable Product Terms. If they are used to transfer personal data to Facebook, Inc. in countries outside the EU or Switzerland and you reside in the European Union or Switzerland, you acknowledge that the Privacy Shield Terms of Use (<https://www.facebook.com/legal/privacyschildtermsforadvertisers>) apply to such data in addition to the applicable Product Terms of Use.

2. Definitions: For the purposes of these Data Processing Terms, the following terms shall have the meanings set out below:

"GDPR" stands for the General Data Protection Regulation (Regulation (EU) 2016/679).

"controller", "processor", "data subject", "personal data", "personal data breach" and "processing" shall have the same meanings as in the GDPR; "processed" and "processing" shall be interpreted in accordance with the definition of "processing".

The data processing conditions for Facebook Business Tools were updated on 31 August 2020.

The Data Processing Terms and Conditions for Facebook Business Tools as amended on 12 August 2020 and the Data Processing Terms and Conditions for Facebook Business Tools as amended on 31 August 2020 shall form the basis for the findings of fact.

Evaluation of evidence C.6.: The findings made are based on the complainant's submission of 17 August 2020 and the documents submitted therein (Exhibit .102 and Exhibit .104). The cited data processing conditions for Facebook Business Tools as amended.

12 August 2020 and as amended on 31 August 2020 are included in the present file and are known to the Parties.

Furthermore, the findings made are based on an official search of the website

<https://www.facebook.com/legal/terms/dataprocessing/update> (retrieved on 6 March 2023).

C.7. To the Privacy Shield Terms of Use

The Privacy Shield Terms of Use for Facebook Business Tools at <https://www.facebook.com/legal/privacysieldtermsforadvertisers> read as follows on 12 August 2020 (formatting not reproduced 1:1, links not included):

"Privacy Shield Terms of Use

*You acknowledge that the use of certain Facebook services for advertising or measurement (the "Services") may result in Facebook, Inc. ("**Facebook**") receiving data from you (either directly or when acting on behalf of Facebook Ireland Ltd). This is done by relying on the EU-US Privacy Shield or the Switzerland-US Privacy Shield (together "**Privacy Shield**"). To the extent the Privacy Shield applies to the information you provide, and without limiting any agreement between you and Facebook, you acknowledge and agree to the following:*

- *Facebook's Privacy Shield Notice is available at www.facebook.com/about/privacysield and sets out Facebook's certification. In accordance with your obligations in connection with your use of the Services, you agree to, provide persons with adequate and appropriate information about the services.*
- *Facebook may provide data subjects with contact information about you through the Services, allowing them to, among other things, contact you directly to exercise their rights under the Privacy Shield.*
- *Facebook may receive requests or complaints from data subjects and may provide them with an independent mechanism for recourse and dispute resolution. Notwithstanding the foregoing, you will remain responsible for resolving any complaints made to you by Data Subjects (whether made directly to you or to us) regarding your processing of Data Subjects' Personal Data in connection with the Services.*
- *You agree to take all reasonable steps (including those reasonably requested by Facebook) to enable Facebook to comply with its Privacy Shield obligations, including assistance in resolving complaints. In the event of any conflict between these Terms of Use and any other Terms of Use that rely on these Terms of Use, these Terms of Use shall prevail.*

Last updated: 29 September 2017"

On 27 September 2021, a new Facebook contract addendum for the transfer of European data came into force. This can be found at https://www.facebook.com/legal/EU_data_transfer_addendum/update and reads as follows (formatting not reproduced 1:1, links not included):

"

Dieser Vertragszusatz für die Übermittlung europäischer Daten tritt am 27. September 2021 in Kraft. Eine Liste der Unterauftragsverarbeiter von Facebook ist [hier](#) einsehbar.

FACEBOOK CONTRACT ADDENDUM FOR THE TRANSFER OF EUROPEAN DATA

This Treaty Supplement for the transfer of European data will enter into force on 27 September 2021.

*This European Data Transfer Addendum ("**Data Transfer Addendum**") is incorporated by reference into the **Data Processing Terms**. It applies to the extent that Facebook Ireland, as your processor, processes European Data pursuant to the Terms of Use for Covered Products and transfers of such data are made from the EU, EEA, United Kingdom or Switzerland to Facebook, Inc.*

- 1. You acknowledge and agree that Facebook Ireland may transfer European data to Facebook, Inc. to provide the Covered Products in accordance with the Terms of Use for Covered Products and that European data may be transferred to other Facebook sub-processors.*
- 2. Facebook Ireland transfers European data to Facebook, Inc. on the basis of processor-to-processor standard contractual clauses, but reserves the right to use an alternative transfer method recognised by the GDPR and other applicable data protection laws in the EEA, UK and Switzerland (such as an adequacy decision). Onward transfers to Facebook's sub-processors based on the processor-to-processor standard contractual clauses are made on the basis of general authorisation in accordance with the data processing terms and conditions.*
- 3. In order to provide an efficient and coordinated service, all communications with Facebook, Inc. or any other Facebook sub-processor in relation to the Processor to Processor Standard Contractual Clauses will be coordinated and routed through Facebook Ireland to the extent possible.*
- 4. This Data Transfer Addendum shall take precedence over the Terms of Use for Covered Products to the extent of any conflict or inconsistency. By continuing to use or access the Covered Products on or after the effective date of this Data Submission Addendum (or any update to this Data Submission Addendum, as applicable), you agree to be bound by the Data Submission Addendum, as updated from time to time.*
- 5. Any clauses agreed to between you and Facebook, Inc. pursuant to the Data Transfer Addendum effective on 31 August 2020 shall be deemed terminated as of the effective date of this Data Transfer Addendum. You agree that any European data transferred pursuant to the terminated clauses need not be destroyed or returned as a result of the termination of those clauses, but instead will be subject to the Terms of Use set forth in this Data Transfer Addendum.*
- 6. The following definitions apply in this Data Transfer Supplement:*
 - a) "**Covered Product**" means a Facebook product or service to which the Terms of Use for Covered Products apply.*
 - b) "**Terms of Use for Covered Products**" means the terms of use applicable to a Facebook Product or Service to the extent that they specify that Facebook Ireland processes European Data as your processor under the **Data Processing Terms** during the provision of the Product or Service (as such Terms of Use for Covered Products may be updated or replaced from time to time).*
 - c) "**Clauses**" stands for the standard contractual clauses for the transfer of personal data to processors established in third countries approved by the European Commission in its Decision 2010/87/EC of 5 February 2010 (but without the illustrative optional clauses).*
 - d) "**EEA**" stands for the European Economic Area.*
 - e) "**EU**" stands for the European Union.*
 - f) "**European Data**" means the personal information under your sole responsibility that is processed by Facebook Ireland as your processor under the Terms of Use for Covered Products to the extent that the GDPR or EEA, UK or Swiss data protection laws apply to the processing of such data.*

- g) **"Facebook Ireland"** stands for Facebook Ireland Limited.
 - h) A **"Facebook sub-processor"** is a sub-processor contracted to process European data in accordance with the Data Processing Terms and Conditions.
 - i. **"Processor-to-Processor Standard Contractual Clauses"**. (a) Module 3 (Processor-to-Processor) of the standard contractual clauses for the transfer of personal data to third countries under the GDPR approved by the European Commission in its Decision 2021/914 of 4 June 2021; or (b) such other (processor-to-processor) standard contractual clauses for the transfer of personal data to third countries as are recognised under applicable data protection laws in the EU, the EEA, the UK or Switzerland (in each case with any optional clauses chosen by Facebook).
7. For the purposes of this Data Submission Supplement, any capitalised terms shall have the meanings ascribed to them in the Terms of Use for Covered Products unless otherwise specified. References to the Terms of Use for Covered Products, including the Data Processing Terms, refer to their respective updated versions, if any, in accordance with the Terms of Use for Covered Products."

On the website <https://www.facebook.com/about/privacyshield>, at least on 12 August 2020, there was still no information that the second respondent no longer uses Privacy Shield for the transfer of personal data to the US.

Evaluation of evidence C.7.: The findings made regarding data protection terms of use are based on the complainant's submission of 17 August 2020 and were not contested by the respondents.

The finding that on the website <https://www.facebook.com/about/privacyshield> at least on the 12 August 2020 that the second respondent no longer uses Privacy Shield for the transfer of personal data to the USA can be seen from Exhibit .106, which the complainant submitted in his submission of 17 August 2020.

Furthermore, the findings made are based on an official search of the website <https://www.facebook.com/legal/privacyshieldtermsforadvertisers>, https://www.facebook.com/legal/EU_data_transfer_addendum/update and <https://www.facebook.com/about/privacyshield> (each retrieved on 6 March 2023).

C.8. Using Facebook Business Tools on [REDACTED] 12 August 2020

The first respondent is the operator of the website [REDACTED] [REDACTED] When it acts is an online news portal which reports on worldwide topics and in particular on topics related to Austria. The first respondent decides on the content and design of the said website.

In any event, on the cut-off date of 12 August 2020, the first respondent took the decision to implement the Facebook business tools "Facebook Login" and "Facebook Pixel" on its website in order to use the tools' functions. For this purpose, it has implemented a JavaScript code that

provided by the second respondent was incorporated into the source text of its website.

[REDACTED]
The respondent to the first complaint has not complied with the terms of use for Facebook Business Tools as amended.

26 December 2019 and the Data Processing Terms and Conditions for Facebook Business Tools as amended.

12 August 2020. The terms and conditions are always concluded between the client (e.g. website operator) and Meta Ireland.

For Facebook Pixel, the first respondent has set up an account ("dashboard") with the tracker ID [REDACTED] with the second respondent. However, the first respondent currently no longer has access to its Facebook Pixel Dashboard.

In any case, the first respondent had used the aforementioned Facebook Business Tools on the cut-off date.

25 October 2022 removed from the [REDACTED] website removed.

Evaluation of evidence C.8.: The findings on the implementation of the Facebook Business Tools on and [REDACTED] the "Dashboard" are based on the first respondent's statement of 7 March 2022, in which it explicitly stated that it had implemented the Facebook Business Tools Facebook Login and Facebook Pixel on the website at least on 12 August 2020 and that the corresponding agreements had been accepted.

were subsequently removed from the aforementioned website also results from the statement of the first respondent of 7 March 2022, which was not disputed by the complainant. An official search by the data protection authority of the website [REDACTED] revealed that the aforementioned Facebook Business Tools are currently no longer used [REDACTED] (queried on 6 March 2023).

The finding that the terms and conditions are always concluded between the client (e.g. operator of a website) and Meta Ireland is based on the credible testimony of the second respondent during the oral hearing on 16 May 2022 (answer to questions 1 and 2).

C.9. Complainant's website visit on 12 August 2020

The complainant visited the website at least on 12 August 2020 [REDACTED] During the visit, he was logged into his Facebook account, which is linked to his email address. The [REDACTED] complainant used the Facebook login function on [REDACTED] not used on 12 August 2020.

Evaluation of evidence C.9.: The [REDACTED] made [REDACTED] findings are based on [REDACTED] the submission of the complainant of 17 August 2020 and are undisputed.

C.10. Data transfers to the USA as a result of the website visit on 12 August 2020

On the occasion of the complainant's visit [REDACTED], as a consequence of the Implementation of Facebook Business Tools on the aforementioned website, on 12 August 2020 at least the following transactions were carried out and the following cookies were set (extract from HAR file, Exhibit ./5):

[REDACTED]

General

Request URL *https://www.facebook.com/tr/*

Request Method *GET*

HTTP

[REDACTED]

HTTP/2 Remote Address

Headers

- **Accept:** *image/webp,*/**
- **Accept-Encoding:** *gzip, deflate, br*
- **Accept-Language:** *en-US,de;q=0.7,en;q=0.3*
- **Connection:** *keep-alive*
- **Cookie:** [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
- **Host:** *www.facebook.com*
- **Referrer:** [REDACTED]
- **TE:** *Trailers*
- **User-Agent:** *Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:79.0) Gecko/20100101 Firefox/79.0*

Query Arguments

- **coo:** *false*
- **dl:** [REDACTED]
- **ec:** *0*
- **ev:** *PageView*
- **fbp:** [REDACTED]
- **id:** [REDACTED]
- **if:** *false*
- **it:** [REDACTED]
- **o:** *30*
- **r:** *stable*

- **rl:** [REDACTED]
- **rqm:** GET
- **sh:** 1080
- **sw:** 1920
- **ts:** [REDACTED]
- **v:** 2.9.23

Cookies

- **_fbp**
 - Value: [REDACTED]
 - Path: /
 - Expires: Session
- **c_user**
 - Value: 1810994287
 - Path: /
 - Expires: Session
- **datr**
 - Value: [REDACTED]
 - Path: /
 - Expires: Session
- **fr**
 - Value: [REDACTED]
 - Path: /
 - Expires: Session
- **locale**
 - Value: en_US
 - Path: /
 - Expires: Session
- **presence**
 - Value: [REDACTED]
 - Path: /
 - Expires: Session
- **sb**
 - Value: [REDACTED]
 - Path: /
 - Expires: Session
- **spin**
 - Value: [REDACTED]
 - Path: /
 - Expires: Session
- **wd**
 - Value: [REDACTED]
 - Path: /
 - Expires: Session
- **xs**
 - Value: [REDACTED]
 - Path: /
 - Expires: Session"

The content of the cited Exhibit ./5 (HAR file) is used as a basis for the findings of fact.

As part of these transactions, due to the implementation of Facebook Pixel on 12 August 2020 at least [REDACTED] the IP address, web browser information,

storage location of the website, pixel-specific data (pixel ID) and click data for buttons of the complainant's end device are transmitted to the second respondent's servers in the USA.

In the context of this transaction, due to the implementation of Facebook Login on 12 August 2020, at [REDACTED] least the following data of the complainant's terminal device was transmitted to the second respondent's servers in the USA:

- IP address;
- User agent;
- Mobile operating system and browser;
- Information about the host server (i.e. the website that contains the login feature);
- Date and time of the website visit;
- Language of the content (i.e. the language of the audience for which the website in question is intended);
- Locale (i.e. usually the country code that refers to the Content-Language field in the HTTP header, e.g. "en-US" versus "en-GB");
- HTTP Referrer (i.e. the URL of the page the person is on);
- Viewport data (i.e. the screen resolution of the device display);
- User ID;
- Cached Access Tokens;
- Standard HTTP Request Headers not already listed; and
- Stored values in FB cookies.

The second respondent can access this data in plain text.

Evaluation of evidence C.10.: The findings made concerning the transactions were based on the complainant's submission of 17 August 2020 and the enclosure .15 (HAR file) submitted therein. A HAR file is an archive format for HTTP transactions. The HAR file was reviewed by the data protection authority. The complainant's allegations are consistent with the archive data contained therein. The HAR file submitted (or its content) is known to the parties. The second respondent also stated in its supplement to the statement of 30 May 2022 entitled "Confidential" that it contains various information (at least the IP address, information on the web browser, location of the website, pixel-specific data (pixel ID) and click data for buttons), at least with regard to Facebook Login.

The finding that the data were transferred to the second respondent's servers in the USA is apparent from the second respondent's statement of 30 May 2022 and the attached data field list (entitled "Confidential"). Although the second respondent states that it receives this data "under the SDK" (apparently meaning: standard data protection clauses), there is no factual reason to assume that it did not also already receive this data on 12 August 2020. Apart from that, certain data, such as the IP address and data on the web browser, are always transmitted when a website is called up. The first respondent also did not dispute the transfer of data to the USA, whereby it did not disclose any data in the context of its

data protection accountability (see the legal assessment and the cited ECJ case law) bears the burden of proof for its arguments.

The finding that pixel-specific data is also transmitted when Facebook Pixel is implemented results from an official search of the website <https://developers.facebook.com/docs/meta-pixel/> (queried on 6 March 2023).

The finding that the Second Respondent can access this data in plain text is based on its statements during the oral hearing of 16 May 2022. Although the Second Respondent did not provide a specific answer to the question of whether it receives the data in plain text as part of the commissioned processing (see question 13). However, it has stated that it provides several services to Meta Ireland, such as infrastructure services, peering, hosting and related services such as testing, bug-fixing as regards Meta Ireland's products, and product security, including investigation of suspicious activities (see Question 11). These services cannot be provided, in the view of the DPA, if the second respondent does not receive the data from Meta Ireland in plain text. Also in the Meta Group Transparency Report at <https://transparency.fb.com/data/government-data-requests/further-asked-questions/> (queried on 6 March 2023) is used as a "protective measure" a "Encryption of data in transit" (i.e. encryption of data in transit), but not effective encryption vis-à-vis the second respondent.

It is not overlooked that other data can be transmitted when Facebook Pixel is implemented on a website, such as click data for buttons. However, the complainant stated in his statement of 25 July 2022 that he had not interacted with Facebook Login. Nor did he otherwise claim to have clicked on Facebook buttons. There were therefore no findings to be made in relation to click data for buttons.

C.11. On the cookies in the specific case

At least the cookie "_fbp" contains a unique, randomly generated value (random number).

The following information on the cookie "_fbp" can be found at https://developers.facebook.com/docs/marketing-api/conversions-api/parameters/fbp-and-fbc/?locale=en_DE (formatting not reproduced 1:1, excerpt, original in English):

fbp

When the Meta Pixel is installed on a website, and the Pixel uses first-party cookies, the Pixel automatically saves a unique identifier to an `_fbp` cookie for the website domain if one does not already exist.

The `fbp` event parameter value must be of the form `version.subdomainIndex.creationTime.randomnumber`, where:

- `version` is always this prefix: `fb`
- `subdomainIndex` is which domain the cookie is defined on ('com' = 0, 'facebook.com' = 1, 'www.facebook.com' = 2). If you're generating this field on a server, and not saving an `_fbp` cookie, use the value 1.
- `creationTime` is the UNIX time since epoch in milliseconds when the `_fbp` cookie was saved. If you don't save the `_fbp` cookie, use the timestamp when you first observed or received this `fbp` value.
- `Randomnumber` is generated by the Meta Pixel SDK to ensure every `_fbp` cookie is unique.

Here's an example of what the `fbp` value could look like:

```
fb.1.1596403881668.1116446470
```

For the cookies `"_fbp"`, `"c_user"`, `xs` and `fr`, the following further information can be found at <https://de-de.facebook.com/policies/cookies/> (formatting not reproduced 1:1, excerpt, emphasis on the part of the data protection authority):

"Authentication"

We use cookies to verify your account and to determine when you are logged in so that we can facilitate your access to the Meta Products and provide you with the appropriate user experience and features.

*For example: We use cookies to help you stay signed in as you move between Facebook pages. Cookies also help us recognise your browser so you don't have to keep signing in to Facebook and so you can sign in to Facebook more easily through third-party apps and websites. For example, including for this purpose, we use **"c_user"** and **"xs"** cookies, which have a 365-day retention period.*

[...]

Advertising, recommendations, insights and measurements

We use cookies as a support to show advertisements about and make recommendations to those people who may be interested in the products, services or purposes advertised by businesses and other organisations.

*For example, cookies allow us to show ads to people who have previously visited a company's website, purchased its products or used its apps, and recommend products and services to them based on that activity. Cookies also allow us to limit the frequency with which you are shown an advert so that you do not see the same advert again and again. The **"fr"***

Cookie is used, for example, to deliver advertisements and to measure and improve their relevance. It has a storage time of 90 days.

We also use cookies to help companies using the Meta Products measure the success of their advertising campaigns.

*For example: We use cookies to determine how often an ad is displayed and to calculate the cost of those ads. We also use cookies to measure how often people take actions, such as making a purchase, after an ad impression. For example, the "**fbp**" cookie identifies browsers to provide analytics services for advertising and websites. It has a retention period of 90 days. [...]"*

Evaluation of evidence C.11.: The findings made are based on an official search of the website https://developers.facebook.com/docs/marketing-api/conversions-api/parameters/fbp-_____and-fbc/?locale=en_DE as well as <https://de-de.facebook.com/policies/cookies/> (retrieved on 6 March 2023).

C.12. To the transparency report of the Meta Group

The Meta Group publishes transparency requests/[transparency reports](https://transparency.fb.com/data/government-data-), including those related to U.S. government data requests, on its website <https://transparency.fb.com/data/government-data->.

The transparency reports show, among other things, that the Meta Group regularly receives data access requests from US secret authorities. The data access requests also concern users from Austria.

Official requests for user data include both routine requests in connection with legal proceedings and urgent disclosure requests. The following data can be requested, among others:

- Basic subscriber information: Name, duration of use, payment information, email addresses and IP addresses of the last logins and logouts.
- Records related to account activity, such as message headers and IP addresses.
- The stored contents of an account, such as messages, photos, videos, timeline entries and location information.

Excerpts from the reports are as follows (formatting not reproduced 1:1, original in English):

"Global Overview

Meta responds to government requests for data in accordance with applicable law and our terms of service. Each and every request we receive is carefully reviewed for legal sufficiency and we may reject or require greater specificity on requests that appear overly broad or vague. This chart provides data on the number of requests we received and the rate we complied with all or some of the government's requests.

request for each half by country or region. We publish this information in 6-month increments, subject to certain limitations, and we began reporting this information in 2013."

[...]

[Home](#) → [Data](#) → [Government Requests for User Data](#)

Data types

Government requests for user data include both routine legal process and emergency disclosure requests. For both request types, we report the number of requests received, the number of users/accounts requested, and the percentage of requests where we produced some data. We have reported this information since 2016.

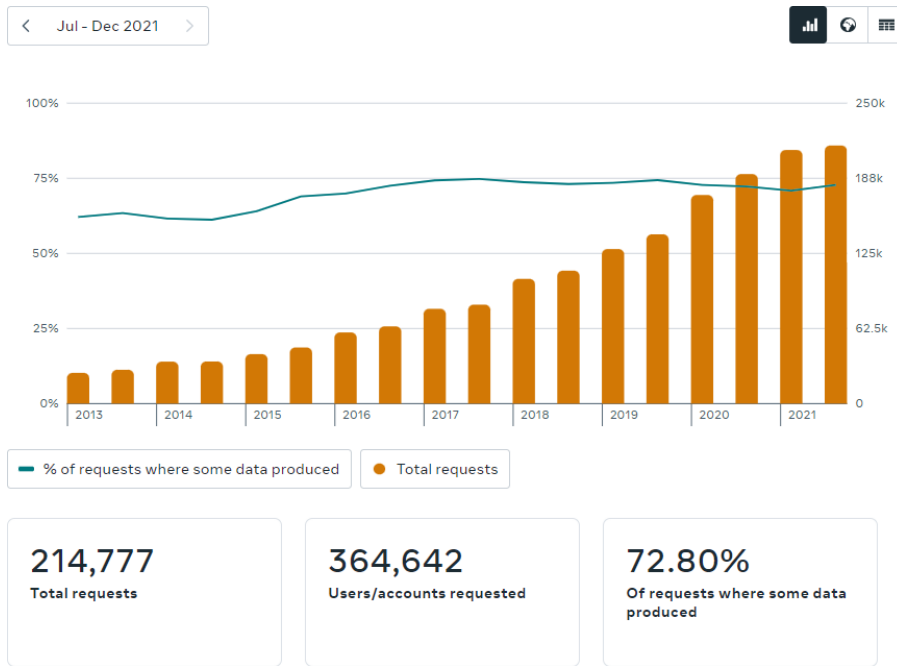
^ Legal process requests

Requests from governments that are accompanied by legal process, like a search warrant. We disclose account records solely in accordance with our Terms of Service and applicable law.

^ Emergency disclosure requests

In emergencies, law enforcement may submit requests without legal process. Based on the circumstances, we may voluntarily disclose information to law enforcement where we have a good faith reason to believe that the matter involves imminent risk of serious physical injury or death.

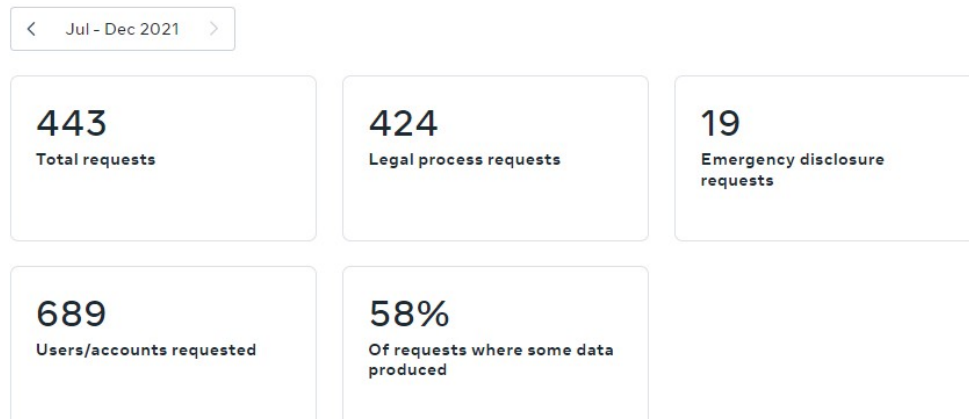
[...]



[...]

Österreich

Facebook responds to government requests for data in accordance with applicable law and our terms of service. Each and every request we receive is carefully reviewed for legal sufficiency and we may reject or require greater specificity on requests that appear overly broad or vague. The charts below provide data on the number of requests we received, the number of users/accounts requested, and the rate we complied with all or some of the government's request.



[...]

^ **Does Meta provide data in response to US government requests?**

Your data may be subject to requests by US government agencies (including US national security authorities) when you use our products and services. We have robust policies to ensure every government request is scrutinized no matter which government makes the request. Meta must comply with valid and compulsory legal requests from US government agencies. These requests must be made in accordance with applicable law and our policies (including [Meta's Data Policy](#)), and we produce only the information that is narrowly tailored to respond to each request.

[...]

Our data disclosure process

^ **What data does Meta disclose in response to government requests?**

Meta scrutinizes every government request and produces only the information that is narrowly tailored to respond to each request. Depending on the request, Meta may produce:

Basic subscriber information: Such as name, length of service, payment information, email addresses, and recent login/logout IP addresses.

Records pertaining to account activity: Such as message headers and IP addresses.

The stored contents of an account: Such as messages, photos, videos, timeline posts, and location information.

For additional information on data we disclose in response to government requests, please see our [guidelines for government requests](#).

On the question of what protective measures are taken to protect data in the context of transfers to the USA, the following information can be found at <https://transparency.fb.com/data/government-data-requests/further-asked-questions/> on the cut-off date of 25 October 2022 (formatting not reproduced 1:1):

"We have in place a number of safeguards and measures to ensure an adequate level of protection for user data being transferred outside the EEA to the United States, including:

Security: We have a comprehensive security program to protect the data stored on our systems, platforms and products.

Encryption of data in transit so it cannot be read: Meta employs industry standard encryption algorithms and protocols designed to secure and maintain the confidentiality of data in transit over public networks. Employing advanced encryption algorithms enables Meta to secure user data in transit from access by third parties.

Policies and procedures: We have robust policies and procedures in place to ensure user data is adequately protected in relation to requests from governmental agencies. For example, we will only comply with a governmental request for user data after we are satisfied that the request complies with applicable law and our policies. If the request is unlawful (for example, overly broad, or legally deficient)

in any way), we will push back or challenge the request. We encourage governmental agencies to submit only requests that are necessary, proportionate, specific, and strictly compliant with applicable laws, by publishing guidelines for government requests.

Oversight: We have a dedicated, trained Law Enforcement Response Team (LERT) that reviews and evaluates every government request for user data individually, whether the request was submitted related to an emergency or through legal process obtained by law enforcement or national security authorities. This team ensures that all requests are consistent with applicable law and our policies, including Meta's Data Policy.

Government Requests for User Data Report: We publish information on government requests we receive in our Government Requests for User Data Report. Information regarding requests made under the US Foreign Intelligence Surveillance Act (FISA) is included in the report with the maximum level of detail permitted under US law.

Advocacy: We appreciate the focus of governments across the globe on protecting and safeguarding people's data, including in the US and Europe, and we work hard to do our part. We actively engage with governments to encourage practices that protect peoples' rights. We belong to advocacy groups like Global Network Initiative, whose mission is to advance the freedom of expression and privacy rights of Internet users worldwide; and are a founding member of Reform Government Surveillance, which advocates for government data requests to be rule bound, narrowly tailored, transparent, subject to strong oversight and protective of end-to-end encryption. We support surveillance reform and frequently engage with various government and regulatory bodies to advocate the same.

Your rights: In addition to your rights under EU law, the SCCs and US law, you also have the right to submit a complaint or request to the Privacy Shield Ombudsperson in the United States".

Evaluation of evidence C.12.: The findings made are based on an official search of the website <https://transparency.fb.com/data/government-data-requests/> and <https://www.facebook.com/safety/groups/law/guidelines/> (each retrieved on 6 March 2023).

C.13. Proceedings before the Irish Regulatory Authority

The Irish supervisory authority (Data Protection Commissioner) is currently conducting proceedings on dg. ZI. IN-20-8-1 against Meta Ireland (Meta Platforms Ireland Ltd). The subject of these proceedings is the order to suspend data transfers to the second respondent.

Evaluation of evidence C.13.: The findings made are based on knowledge known to the authorities. Furthermore, in his statement of 25 July 2022, the complainant also referred to the proceedings on dg. ZI. IN-20-8-1.

D. In legal terms, it follows:

D.1. On the competence of the data protection authority

a) On the media privilege pursuant to Section 9 (1) of the Data Protection Act

In its statement of 28 December 2020, the first respondent contested the competence of the data protection authority to deal with the complaint in question, and the

complainant argued Article 9(1) of the Data Protection Act was applicable to the data processing in question, i.e. the transfer of the complainant's personal data as a result of the implementation of Facebook Business Tools at [REDACTED] complainant's personal data was not transferred to Facebook Business Tools

The following is to be countered:

The national legislator restricts the so-called media privilege under Art. 85 GDPR in conjunction with Section 9(1) DPA by making the privilege available only to media companies or media services, provided that personal data are processed for journalistic purposes by media owners, publishers and media employees or employees of a media company or media service. (cf. the decision of the DPA of 21 April 2020, GZ: 2020-0.239.741).

According to the understanding of the ECJ, personal data is processed for journalistic purposes if the processing has the sole purpose of disseminating information, opinions or ideas to the public (cf. the ECJ judgment of 16 December 2008, C-73/07 para. 62).

The extent to which the data processing subject of the complaint pursues a "journalistic purpose" as defined by the ECJ's case law is not apparent. Rather, it is clear from the statement of the first respondent dated 7 March 2022 that Facebook Pixel was implemented for tracking purposes and Face Login was implemented to [REDACTED] simplify the login process for premium customers.

Apart from this, Meta Ireland receives data from website visitors due to the implementation of Facebook Business Tools on a website, which in turn can be processed for its own purposes (see e.g. statement of facts C.4). Thus, with regard to the data transfers between the first respondent and Meta Ireland (and ultimately the second respondent) that are the subject of the complaint, no journalistic purpose within the meaning of the ECJ's case law was pursued for this reason alone.

These considerations are also covered by the case law of the Federal Administrative Court, according to which, for example, advertising cookies for playing personalised advertising on a website of a media company or the administration of a database by a media company for the purpose of sending print advertising are not subject to media privilege (cf. the decision of the Federal Administrative Court of 12 March 2019, GZ: W214 2223400-1).

Since the requirements of Section 9 (1) of the Data Protection Act are not met, the media privilege does not apply to the data processing subject of the complaint.

The (interim) decision of the Constitutional Court of 14 December 2022, Zl. G 287/2022-16, G 288/2022-14, which repealed section 9(1) of the FADP as unconstitutional, does not need to be addressed, as the repeal will not enter into force until 30 June 2024.

b) On the ePrivacy Directive

The European Data Protection Board (hereinafter: EDSA) has already addressed the relationship between the GDPR and Directive 2002/58/EC ("ePrivacy Directive") (see Opinion 5/2019 on the interaction between the ePrivacy Directive and the GDPR of 12 March 2019).

The data protection authority also dealt with the relationship between the GDPR and the national transposition provision (in Austria now: TKG 2021, BGBl. I No. 190/2021 as amended) in its decision of 30 November 2018, GZ: DSB-D122.931/0003 DSB/2018.

In principle, it was stated that the ePrivacy Directive (or the respective national implementation provision) takes precedence over the GDPR as *lex specialis*. Article 95 of the GDPR states that the Regulation does not impose any additional obligations on natural or legal persons with regard to processing in connection with the provision of publicly available electronic communications services in public communications networks in the Union, insofar as they are subject to specific obligations set out in the ePrivacy Directive which pursue the same objective.

However, the ePrivacy Directive does not contain any obligations within the meaning of Chapter V of the GDPR in case of transfer of personal data to third countries or to international organisations.

Against this background, the GDPR applies to such a data transfer.

c) Interim result

The data protection authority is competent to deal with the complaint in question pursuant to Article 77(1) of the GDPR.

D.2. On Art. 44 GDPR as a subjective right

Based on the previous practice of the data protection authority and the courts, it should be noted that both the lawfulness of data processing pursuant to Art. 5(1)(a) in conjunction with Art. 6 et seq. of the GDPR and the data subject rights postulated in Chapter III of the Regulation can be asserted as a subjective right in the context of a complaint pursuant to Art. 77(1) of the GDPR.

In the present case, a violation of Art. 44 GDPR is (also) alleged.

According to the data protection authority, the decisive factor is whether a data subject is adversely affected in an individual legal position by an alleged infringement. The alleged infringement must therefore have a negative impact on the data subject. This can be assumed for Art. 44 GDPR if personal data are transferred to a third country or an international organisation and the level of protection guaranteed by the regulation is undermined (cf. also the ECJ judgment of 16 July 2020, C-311/18 para. 135).

The wording of Article 77(1) of the GDPR (and, incidentally, the national provision of Section 24(1) of the GDPR) also only requires that "*[...] the processing of personal data relating to them infringes this Regulation*" in order to exercise the right of appeal.

In this sense, the ECJ stated in its judgment of 16 July 2020 that the finding that "*[...] the law and practice of a country do not ensure an adequate level of protection [...]*" and "*[...] the compatibility of this (adequacy) decision with the protection of privacy, as well as of the freedoms and fundamental rights of individuals [...]*" may be invoked as a subjective right in the context of a complaint under Article 77(1) GDPR (see the ECJ judgment of 16 July 2020, C-311/18 para 158).

Although it should be noted that the question referred for a preliminary ruling in the above-mentioned proceedings did not concern the "scope of the right of appeal under Article 77(1) of the GDPR", the ECJ obviously considered the fact that a breach of provisions of Chapter V of the GDPR can also be asserted in the context of a complaint under Article 77(1) of the GDPR to be a necessary precondition. Otherwise, the ECJ would have stated that the question of the validity of an adequacy decision cannot be clarified in the context of a complaint procedure.

Finally, also according to the national case law of the Administrative Court, it is to be assumed in case of doubt that norms which prescribe an official procedure also and especially in the interest of the person concerned grant him a subjective right, i.e. a right which can be enforced by way of appeal (cf. e.g. VwSlg. 9151 A/1976, 10.129 A/1980, 13.411 A/1991, 13.985 A/1994).

Thus, a violation of Art. 44 GDPR can be asserted in the context of a complaint to the data protection authority.

D.3. On the declaratory competence of the data protection authority

As can be seen from the subject matter of the complaint (see point B.1), a declaration of a violation of the law, which lies in the past, was requested.

According to the Judicature of the VwGH and of the BVwG comes the data protection authority a declaratory competence in the with regard to on violations of the right to Confidentiality in

appeal proceedings (as explicitly stated in the decision of the Federal Administrative Court of 20 May 2021, ZI. W214 222 6349-1/12E; implicitly the decision of the Administrative Court of 23 February 2021, Ra 2019/04/0054, in which it dealt with the determination of a past violation of the obligation to maintain secrecy without addressing the lack of jurisdiction of the public authority).

There are no factual reasons for not exercising the declaratory competence pursuant to Art. 58 para. 6 DSGVO in conjunction with Art. 58 para. 6 DSGVO.

§ Article 24(2)(5) of the GDPR and Article 24(5) of the GDPR cannot also be used to establish a violation of Article 44 of the GDPR, since in the present case, too, a violation of the law in the past - namely data transfers to the USA on 12 August 2020 - is complained about and the right to complain pursuant to Article 24(1) of the GDPR - as well as Article 77(1) of the GDPR - is generally linked to a violation of the GDPR.

If the decision in an appeal procedure could only contain instructions pursuant to Article 58(2) of the GDPR, there would be no room for Article 24(2)(5) and Article 24(5) of the GDPR.

As far as the first respondent in its statement of 18 October 2022 refers to Section 24 (6) of the FADP and states that the alleged violation of the law has been remedied, it must be countered by the case law of the Federal Administrative Court, according to which the possibility to subsequently remedy a violation of the law pursuant to Section 24 (6) leg. cit. is not possible in the case of violations that have already been committed (and can no longer be remedied) (cf. the decision of the Federal Administrative Court of 29 June 2022, no. W245 2232755-1).

Thus, the data protection authority has the competence to make a determination in the present complaint procedure.

D.4. Re point 1

The data protection authority suspended the proceedings in question by decision of 2 October 2020, no. D155.028, 2020-0.527.429. D155.028, 2020-0.527.429.

Since ex officio decisions from which no right has accrued to anyone can be revoked or amended both by the authority that issued the decision and, in the exercise of the supervisory right, by the relevant higher authority, and no right to non-decision accrues to a party to the proceedings as a result of a stay of proceedings, the above-mentioned decision of 2 October 2020 was also amenable to a remedy pursuant to section 68(2) AVG.

D.5. Re point 2

a) On the term "personal data

According to the legal definition of Art. 4 No. 1 GDPR, "*personal data means any information relating to an identified or identifiable natural person (hereinafter referred to as 'data subject')*".

identifiable means a natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

As can be seen from the findings of fact (see C.8), the first respondent - as operator of the website - implemented Facebook Business Tools on its website. As a result of this implementation - i.e. triggered by the JavaScript code executed when visiting the website - at least the following information of the complainant's terminal device was transmitted to the servers of the second respondent (see C.9):

- IP address;
- User agent;
- Mobile operating system and browser;
- Information about the host server (i.e. the website that contains the login feature);
- Date and time of the website visit;
- Language of the content (i.e. the language of the audience for which the website in question is intended);
- Locale (i.e. usually the country code that refers to the Content-Language field in the HTTP header, e.g. "en-US" versus "en-GB");
- HTTP Referrer (i.e. the URL of the page the person is on);
- Viewport data (i.e. the screen resolution of the device display);
- User ID;
- Cached Access Tokens;
- Standard HTTP Request Headers not already listed; and
- Stored values in FB cookies.

The data protection authority has already stated the following regarding the "Google Analytics" tool in its non-rk decision of 22 April 2022, GZ: 2022-0.298.191 (available at www.dsb.gv.at):

"In the opinion of the data protection authority, there is already an interference with the fundamental right to data protection pursuant to Art. 8 EU-GRC as well as § 1 DSG if certain authorities take measures - in this case the assignment of such identification numbers - in order to individualise website visitors in this way.

A standard of "identifiability" to the effect that it must be immediately possible to associate such identification numbers also with a certain "face" of a natural person - i.e. in particular with the name of the complainant - is not required (cf. in this regard already

the former Art. 29 Working Party's Opinion 4/2007, WP 136, 01248/07/DE on the concept of "personal data" p. 16 f; cf. the supervisory authorities' guidance for telemedia providers from March 2019, p. 15).

Such an interpretation is supported by recital 26 of the GDPR, according to which the question of whether a natural person is identifiable takes into account "[...] any means reasonably likely to be used by the controller or by any other person to identify the natural person, directly or indirectly, such as singling out". Singling out" is understood to mean "picking out from a crowd" (cf. <https://www.duden.de/rechtschreibung/aussondern>, queried on 18 March 2022), which is in line with the above considerations on individualisation of website visitors.

[...]

At this point, it should be noted that the European Data Protection Supervisor (EDPS) also takes the view that "segregation" by marking a terminal device is to be considered as personal data. In his decision of 5 January 2022, Ref. No. 2020-1013, against the European Parliament, the EDPS stated the following:

"Tracking cookies, such as the Stripe and the Google analytics cookies, are considered personal data, even if the traditional identity parameters of the tracked users are unknown or have been deleted by the tracker after collection. All records containing identifiers that can be used to single out users, are considered as personal data under the Regulation and must be treated and protected as such." (p. 13, original in English and with further references).

"[...] Tracking cookies such as the Stripe and Google Analytics cookies are considered personal data, even if the traditional identity parameters of the tracked users are unknown or have been deleted by the tracker after collection. All data sets that contain identifiers that can be used to single out users are considered personal data under the Regulation and must be treated and protected as such" (translation by the DPA).

It is true that the EDPS has to apply Regulation (EU) 2018/1725, which applies to data processing by Union institutions, bodies, offices and agencies. However, since Article 3(1) of Regulation (EU) 2018/1725 corresponds to the definition of Article 4(1) of the GDPR, these considerations can be readily applied to the case at hand."

These considerations can be applied to the case at hand:

As a result of the implementation of Facebook Business Tools, cookies [REDACTED] were set up on end device of the complainant were set, which contain a unique, randomly generated value (see C.11). This makes it possible to individualise the complainant's terminal device and record the complainant's surfing behaviour in order to display suitable personalised advertising (see C.3).

Irrespective of this, at least Meta Ireland had the possibility to link the data it received due to the implementation of Facebook Business Tools on [REDACTED] complainant's Facebook account. It is [REDACTED] clear from the Facebook Business Tools Terms of Use (see C.5) that Facebook Business Tools are used, inter alia, to exchange information with Facebook.

It is not necessary that the first respondent alone must be able to establish a personal link, i.e. that all information necessary for identification is with the first respondent (cf. ECJ judgments of 20 December 2017, C-434/16, para. 31, as well as of 19 October 2016, C-582/14, margin note 43).

These remarks are also covered in *Fashion ID*. In the dg. decision, the ECJ also assumed that the integration of a Facebook "Like" button on a website - irrespective of whether the button is also clicked - triggers a processing of personal data (see the ECJ judgment of 29 July 2018, C-40/17 para 80). From the ECJ's perspective, it was therefore not necessary for the dg. Website operator must be able to establish the personal reference.

The ECJ's statements can be applied to the case at hand, since according to the terms of use, the "Like" button as well as Facebook Login and Facebook Pixel are part of the Facebook Business Tools (see C.5).

Thus, the information listed in the findings of fact under C.10. (at least in combination) is personal data according to Art. 4 Z 1 DSGVO.

b) Distribution of roles

i) Respondent to the first complaint

As already explained, the first respondent as website operator took the decision to implement Facebook Business Tools on its website at the time relevant to the complaint. Specifically, it inserted a JavaScript code provided by the second respondent into the source code of its website, whereby this JavaScript code was executed in the complainant's browser when visiting the website (see C.8).

In its statement of 7 March 2022, the first respondent explained that Facebook Pixel was implemented tracking purposes and Face Login was implemented to simplify the login process for premium customers on [REDACTED] first respondent also explained that Facebook Pixel was implemented tracking purposes.

In doing so, the first respondent decided on the "purposes and means" of the data processing in connection with the tool, which is why it is to be regarded as the controller within the meaning of Article 4(7) of the GDPR.

ii) Second respondent

Despite extensive investigative proceedings - for example, an oral hearing of the second respondent took place on 16 May 2022 - the data protection authority does not currently have sufficient indications to qualify the second respondent as a data controller for the data processing in question.

In accordance with the data processing conditions (see C.6), the data protection authority therefore assumes that the second respondent (then Facebook Inc.) was used as a processor within the meaning of Article 28 (2) of the GDPR in the context of the data processing in question on 12 August 2020.

The question of whether the data access possibilities of US intelligence services change anything about the role of the second respondent is addressed below.

c) Scope of Chapter V GDPR

According to Art. 44 of the GDPR, any "[...] *transfer of personal data which have already been or to be processed after their transfer to a third country or an international organisation [...] shall only be allowed if the controller and the processor comply with the conditions laid down in this Chapter and also with the other provisions of this Regulation, including any onward transfer of personal data from that third country or international organisation to another third country or international organisation. All the provisions of this Chapter shall be applied in order to ensure that the level of protection of natural persons ensured by this Regulation is not undermined.*"

The first respondent is based in Austria and is the data controller for the operation of the website. [REDACTED] Furthermore, the first respondent has disclosed personal data of the complainant by proactively implementing Facebook Business Tools on its website and, as a result of this implementation, has [REDACTED] on its website and, as a result of this implementation inter alia, a data transfer to the second respondent (registered office: USA) took place (see also EDSA Guidelines 5/2021 as amended on 14 February 2023 FN 15: "*Finally, it should be noted that personal data disclosed via cookies are not considered as being disclosed directly by the data subject, but rather as a transmission by the operator of the website that the data subject is visiting*").

It can be left open whether personal data of the complainant were transferred directly to the second respondent or only in a second step after they had been processed by Meta Ireland:

Pursuant to Article 28 (1) of the GDPR, the first respondent is obliged to cooperate only with processors that offer sufficient guarantees that the data processing will be carried out in compliance with the requirements of the GDPR ("selection fault").

According to the established case law of the Federal Administrative Court, the processor is the "extended arm" of the controller and the commissioned processing is to be seen as part of the processing by the controller itself (see the decision of the Federal Administrative Court of 20 October 2021, ZI. W211 2231475-1; also explicitly EDSA Guidelines 5/2021 as amended on 14 February 2023, margin no. 19, last sentence).

In the case at hand, the first respondent accepted Meta Ireland's data processing terms and conditions for Facebook Business Tools and, in accordance with Article 28(2) of the GDPR, consented to Meta Ireland using the second respondent (then Facebook Inc.) as a so-called "data controller".

(see C.6: "[...] You hereby authorise Facebook to engage Facebook Inc. [and other Facebook companies] as its sub-processor(s)").

d) Set of rules of Chapter V GDPR

Subsequently, it must be examined whether the data transfers to the USA that are the subject of the complaint took place in accordance with the provisions of Chapter V of the GDPR.

Chapter V of the Regulation provides for three (protection) instruments to ensure the adequate level of protection required by Art. 44 GDPR for data transfers to a third country or an international organisation:

- Adequacy decision (Art. 45 GDPR);
- Appropriate safeguards (Art. 46 GDPR);
- Exceptions for certain cases (Art. 49 GDPR).

e) Adequacy decision

As can be seen from the findings of fact (see C.6 and C.7), the respondents invoked the EU-US adequacy decision ("Privacy Shield") for the data transfer on 12 August 2020.

However, the ECJ has already pronounced on 16 July 2020, C-311/18, that the EU-US Adequacy Decision does not ensure an adequate level of protection for individuals due to the relevant US law and the implementation of regulatory surveillance programmes - based, inter alia, on Section 702 of FISA and E.O. 12333 in conjunction with PPD-28 - do not ensure an adequate level of protection for individuals (ibid. para. 180 et seq.) and has declared the EU-US adequacy decision invalid - without upholding its effect (ibid. para. 201 et seq.).

According to the DPA, the Second Respondent also qualifies as an electronic communications service provider within the meaning of 50 U.S.Code § 1881(b)(4) and is thus subject to surveillance by U.S. intelligence agencies under 50 U.S.Code § 1881a ("FISA 702").

Accordingly, the second respondent has the obligation to notify the US authorities under 50 U.S. Code § Section 1881a to provide personal data. The Meta Group's transparency report (see C.12) shows that the US secret authorities regularly make such requests.

(ii) appropriate guarantees

As can be seen from the findings of fact (see C.7), the Facebook contract addendum (including the conclusion of standard data protection clauses) was only implemented after 12 August 2020.

ii) Exceptions for certain cases

The respondents did not rely on Art. 49 GDPR at any point in the investigation procedure.

From the perspective of the data protection authority, no facts of Art. 49 GDPR are fulfilled and, in particular, no consent pursuant to Art. 49 (1) lit. a leg. cit. was obtained (cf. the ECJ ruling of 27 October 2022, C-129/21 para. 81 et seq. on the burden of proof of a controller in this regard).

f) Result

The data transfers at issue on 12 August 2020 were not covered by any of the instruments of Art. 45 et seq. of the GDPR.

Therefore, a violation of Art. 44 of the GDPR had to be established according to the ruling.

D.6. Re point 3

a) Concerning grievance A)

It must be examined whether the second respondent (as data importer) is also subject to the obligations standardised in Chapter V of the Regulation.

Based on the EDSA Guidelines 5/2021 as amended on 14 February 2023, it should be noted that a "transfer to a third country or an international organisation" within the meaning of Art. 44 GDPR only exists if, inter alia, the controller or processor (data exporter), by transfer or otherwise, transfers personal data which are the subject of this

processing is disclosed to another controller, a joint controller or a processor (data importer) (ibid. para. 9).

This requirement does not apply to the second respondent in the present case, as it (as data importer) does not disclose the complainant's personal data, but (only) receives it.

It is true that the data protection authority does not overlook the fact that a data transfer necessarily presupposes a recipient and that the second respondent is part of the data transfer (at least from a technical point of view). However, it must be countered that the data protection responsibility in a processing operation can nevertheless be "shared" (from a legal point of view), i.e. there can be a different degree of responsibility depending on the phase of the processing operation (cf. the EDSA Guidelines 7/2020 on the concept of controllers and processors, margin no. 63 et seqq).

In the opinion of the data protection authority, there is therefore no violation of Article 44 of the GDPR by the second respondent.

b) Re grievance B)

Finally, a violation of Art. 5 et seq, Art. 28, and Art. 29 of the GDPR by the second respondent must be examined. In this regard, the complainant argues that the second respondent processed his data contrary to the instructions and requests of the first respondent.

The following is to be countered:

The data protection principles and the requirements for the lawfulness of data processing pursuant to Art. 5 et seq. of the GDPR are, according to the explicit wording of Art. 5 para. 2 leg. cit. an obligation of the controller.

However, in the opinion of the data protection authority, the (mere) possibility that the second respondent becomes the addressee of enquiries by the US security authorities does not automatically lead to its responsibility under Article 28 (10) of the GDPR. Such a broad interpretation of Article 28 (10) of the GDPR seems too expansive.

Moreover, a violation of Art. 28 and Art. 29 GDPR cannot be asserted as a subjective right insofar as the cited provisions (only) regulate the relationship between the controller and the processor and a violation by the processor is attributable to the controller (cf. again the decision of the BVwG of 20 October 2021, ZI. W211 2231475-1).

However, these remarks do not play a role for headnote 2, since in the context of a violation of Art. 44 GDPR, the success of the complaint is already fulfilled if personal data are transferred to the USA without a protection instrument.

The decision was therefore in accordance with the ruling.

RECORDING MEASURES

An appeal against this decision may be filed in writing with the Federal Administrative Court within **four weeks** after service. The appeal **must be lodged with the data protection authority** and must

- the designation of the contested decision (GZ, subject)
- the designation of the authority against which proceedings have been brought,
- the grounds on which the allegation of illegality is based,
- the request and
- contain the information necessary to assess whether the complaint has been filed in time.

The data protection authority has the option of either amending its decision within two months by means of a **preliminary appeal decision** or **submitting** the appeal with the files of the proceedings to **the Federal Administrative Court**.

The appeal against this decision is **subject to a fee**. The fixed fee for a corresponding submission including enclosures is **30 euros**. The fee is to be paid to the account of the Tax Office Austria, stating the purpose of use.

The fee must always be transferred electronically using the function "Finanzamtszahlung". The Austrian Tax Office - Special Responsibilities Department must be indicated or selected as the recipient (IBAN: AT83 0100 0000 0550 4109, BIC: BUNDATWW). Furthermore, the tax number/levy account number 10 999/9102, the levy type "EEE complaint fee", the date of the notice as the period and the amount are to be indicated.

If the e-banking system of your credit institution does not have the "tax office payment" function, the eps procedure in FinanzOnline can be used. An electronic transfer can only be dispensed with if no e-banking system has been used so far (even if the taxpayer has an internet connection). In this case, the payment must be made by payment order, whereby attention must be paid to the correct allocation. Further information is available from the tax office and in the manual "*Electronic payment and notification for payment of self-assessment levies*".


The payment of **the fee** shall be **proven to the data protection authority upon** submission of the complaint by means of a payment voucher to be attached to the submission or a printout showing that a payment order has been issued. If the fee is not paid or not paid in full, the **competent tax office** shall be **notified**.

A timely and admissible appeal to the Federal Administrative Court has a **suspensive effect**. The suspensive effect may have been excluded in the ruling of the decision or may be excluded by a separate decision.

6 March 2023

For the head of the data protection authority:



	Signatory	serialNumber=1831845058,CN=Data Protection Authority,C=AT
	Date/Time	2023-03-06T13:08:52+01:00
	Test information	Information on the verification of the electronic seal or electronic signature can be found at: https://www.signaturpruefung.gv.at Information on how to check the printout can be found at: https://www.dsb.gv.at/-/amtssignatur
	Note	This document has been officially signed.