REPUBLIC OF CYPRUS

OFFICE OF THE COMMISSIONER
FOR PERSONAL DATA PROTECTION

MACHINE TRANSLATED

Case Reg.: 11.17.001.008.229

DECISION

Complaint of a personal data breach

In the light of the tasks and powers conferred on me by Article 57(1)(f) of Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter referred to as "the Regulation"), I have examined a complaint lodged at my Office, pursuant to Article 77(1) of the Regulation, against "ARKTINOS" Publications Ltd ("Politis" newspaper) (hereinafter the "defendant"); Facebook Ireland Ltd (hereinafter "Facebook Ireland") and Facebook Inc. The complaint was lodged with the Austrian Data Protection Supervisory Authority on 17 August 2020 by a resident of Austria (hereinafter the "complainant"), represented, pursuant to Article 80(1) of the Regulation, by the non-profit organisation noyb – European Centre for Digital Rights.

On the basis of the investigation, I have found an infringement of the Regulation by the defendant and therefore adopt this Decision.

A. Facts of the case

Positions of the Complainant

2. The complaint relates to an alleged breach of the provisions of Chapter V of the Regulation. The complaint states inter alia that:
2.1. the complainant, on 12 August 2020, at 11:43 a.m., visited the website https://politis.com.cy (hereinafter the "website") while logged in to a Facebook account with his e-mail address,

2.2. the defendant has integrated HTML code for Facebook Services (including Facebook Connect).

2.3. during the complainant's visit to the website, the defendant processed the complainant's personal data (at least the IP address and cookie data), of which at least some were transferred to Facebook Inc, in the United States. The complainant does not have the technical means to determine whether such data transfer took place directly between defendant and Facebook Inc. or via Facebook Ireland as an intermediary,

2.4. Facebook Connect is a service used by third party websites, enabling the flow of user's personal data between the site and Facebook;

2.5. the use of Facebook Connect was subject, when submitting the complaint, to the documents Facebook Business Tools Terms and Facebook Data Processing Terms. These two documents would be updated with effect from 31 August 2020 (New Facebook Business Tools Terms and New Facebook Data Processing Terms);

2.6. interpreting the Facebook Business Tools Terms and Facebook Data Processing Terms, which were in force at the time of the complaint, it is concluded that:
2.6.1. Facebook Ireland is the contractual partner of the controller and acts as processor in accordance with Article 4(8) of the Regulation,
2.6.2. Facebook Inc. acts as a sub-processor.

This conclusion is also apparent from the New Facebook Business Tools Terms and New Facebook Data Processing Terms.

2.7. in any case, the complainant's personal data has been transferred by the defendant in the United States. This transfer, by the defendant, which is an EEA-based company, to Facebook Inc. or to any other processor in the United States (or to any other country outside the EEA) requires a legal basis in accordance with Article 44 of the Regulation;

2.8. as the CJEU has annulled the EU-US Privacy Shield in judgment C-311/18, the controller can no longer base the transfer of data to Facebook Inc. on an adequacy decision under Article 45 of the Regulation;

2.9. however, the Facebook team and the controller are still trying to base the transfer on the invalidated "EU-US Privacy Shield", as evidenced by point 4 of the Facebook Data Processing Terms:
Facebook, Inc. has made commitments under the EU-U.S. Privacy Shield and Swiss-U.S. Privacy Shield that may apply to data transferred by you or Facebook Ireland Limited to Facebook, Inc. under the Applicable Product Terms. When applicable as the means to transfer Personal Data outside of the EU or Switzerland to Facebook, Inc. where you are in the European Union or Switzerland, you acknowledge that the Privacy Shield Terms (https://www.facebook.com/legal/privacyshieldtermsforadvertisers) apply to such data in addition to the Applicable Product Terms.';

2.10. regarding these data transfers, the Facebook Data Processing Terms contains a link and reference to Privacy Shield Terms, which in turn is linked to Facebook Inc. and the EU-U.S. and Swiss-U.S. Privacy Shield.

2.11. a similar reference can be found in the New Facebook Data Processing Terms document, which would be implemented 6 weeks after the CJEU's ruling:
Facebook, Inc., which is used by Facebook Ireland as a sub-processor, has made commitments under the EU-U.S. Privacy Shield and Swiss-U.S. Privacy Shield that may apply to Personal Information transferred by you or Facebook Ireland to Facebook, Inc. under the Applicable Product Terms. When applicable as the means to transfer Personal Information outside of the EU/EEA or Switzerland to Facebook, Inc., you acknowledge that the Privacy Shield Terms apply in addition to the Applicable Product Terms.';

2.12. a regular data transmission system based on an annulled adequacy decision constitutes a serious, systematic and, in view of the New Facebook Data Processing Terms, an intentional violation of Article 45 and subsequent articles of the Regulation;

2.13. nor can the controller base the transfer of data on standard contractual clauses, in accordance with Article 46(2)(c) and (d) of the Regulation, if the third country does not ensure adequate protection of personal data transferred in accordance with these clauses, under EU law. The CJEU explicitly found that onward transfer to companies falling under 50 U.S. Code § 1881a, not only violates the relevant articles of Chapter V of the Regulation, but also Articles 7 and 8 of the EU Charter of Fundamental Rights, as well as the substance of Article 47 of the Charter (C-362/14 ("Schrems I"), para. 95). Therefore, any onward transfer violates the fundamental right to privacy, data protection and the right to effective judicial protection and a fair trial;

2.14. Facebook Inc. qualifies as a provider of electronic communications services within the meaning of 50 U.S. Code § 1881(b)(4) and is therefore subject to U.S. intelligence surveillance under 50 U.S. Code § 1881a ("FISA 702"). As evidenced by the Snowden Transparencys and the Facebook Transparency Report (https://transparencyreport.google.com/userdata/us-national-security), Facebook Inc. actively provides personal data to the U.S. Government pursuant to 50 U.S. Code § 1881a;

2.15. consequently, the controller is not in a position to ensure adequate protection of the complainant's personal data transferred to Facebook Inc. Therefore, the controller has a legal obligation to refrain from transferring the complainant's data – or any other personal data – to Facebook Inc. However, for more than one month after the decision, the controller has not acted on the basis of the decision,

2.16. the Facebook group continues to accept data transfers from the EU/EEA, both on the basis of the invalidated "EU-US Privacy Shield" and standard contractual clauses, despite the CJEU's clear judgement and violation of Articles 44 to 49 of the Regulation. Facebook Inc. further discloses personal data from the EU/EEA to the U.S. government, in violation of Article 48 of the Regulation.

2.17. in accordance with Article 3(2)(a) of the Regulation, the Regulation is extended to sub-performers, who are not established in the Union, where the processing activities relate to the offering of services to data subjects in the Union. Consequently, there is direct jurisdiction against Facebook Inc. While Facebook Ireland may claim to fall under the jurisdiction of the Supervisory Authority of Ireland, as the lead Supervisory Authority (Article 56 of the Regulation), there is no main establishment of Facebook Inc. in the Union. Therefore, any Data Protection Authority of the Union has direct jurisdiction over Facebook Inc., under its sub-processor activities,

2.18 pursuant to Articles 58 and 83 of the Regulation, the competent Supervisory Authority may use corrective and sanctioning powers against both the controller and the processor Facebook Ireland and the underprocessor Facebook Inc.,

2.19. in accordance with the above CJEU ruling, the competent Supervisory Authority must suspend or terminate the transfer of personal data to the third country, pursuant to Article 58(2)(f) and (j) of the Regulation;

2.20. the complainant requests that:
2.20.1. the complaint under Article 58 of the Regulation has been fully investigated and clarified:

(a) what personal data has been transferred by defendant and/or Facebook Ireland to Facebook Inc. in the United States or to any other third country or international organisation;
(b) on which transfer mechanism the defendant and/or Facebook Ireland based the transfer of data;
(c) whether the provisions of the Facebook Business Tools Terms and Facebook Data Processing Terms, at the time of lodging the complaint and as to be amended as from 31 August 2020, met the requirements of Article 28 of the Regulation concerning the transfer of personal data to third countries;

2.20.2.immediately prohibit or suspend any transfer of data by defendant and/or Facebook Ireland to Facebook Inc. in the United States, and order the data to be returned to the EU/EEA or another country providing adequate protection pursuant to Article 58(2)(d), (f) and (j) of the Regulation;

2.20.3.an effective, proportionate and dissuasive fine shall be imposed on the defendant, Facebook Ireland and Facebook Inc. pursuant to Article 83(5)(c) of the Regulation, taking into account that:
(a) the complainant is probably only one out of thousands of users (Rule 83(2)(a) of the Rules of Procedure);
(b) at the time of the complaint, more than a month had elapsed since judgment C-311/18 of the CJEU and the defendant did not take any measures to bring the processing operations into compliance with the provisions of the Regulation (Rule 83(2)(b) of the Rules of Procedure).

Where reference is made to the controller above, the defendant is understood.

Positions of the Defendant

3. As part of the investigation of the complaint, my Office sent a letter to the defendant with clarification questions on 23 December 2020. This letter was sent again to the defendant on 7 January and 18 February 2021.

4. In a letter dated 18 February 2021, the defendant submitted the reply of the technician, who developed the website. In particular, it was mentioned that to the best of his knowledge, there were no specific codes on the site, as “login with facebook etc” was never used. However, the relevant questionnaire sent was not answered.

5. On 20 January 2022, my Office sent a new letter to the defendant, and after it was reiterated that, based on the analysis of the data and file submitted by the complainant, as well as an audit on the website, a Facebook tool was used, new questions were asked and the questions contained in the Office’s letter of 23 December 2020 requested to be answered.

6. In a letter dated 26 January 2022, the defendant stated inter alia the following:
6.1. as regards the questions contained in my Office’s letter of 23 December 2020 concerning the Facebook Connect tool, it was already mentioned in the letter dated 18 February 2021 that the Facebook Connect tool is not used. However, the technical developer of the website was contacted again, who confirmed that this tool was never used on the website. A user chooses to access a third-party website through Facebook Connect,

they allow that website to retrieve information they have given to Facebook, including their full name, pictures, wall posts, friend information, etc.. It was stated that the defendant never had access to such sensitive information, let alone to process it,

6.2. the Facebook tools that were, and still were, at the time of submitting the reply, are the Facebook domain verification and the Facebook pixel.
6.2.1. Facebook domain verification is a tool for website validation purposes, to avoid blocking from the platform, in cases of spam reporting, and

6.2.2. the Facebook pixel tool is a tool for paid ads ("paid ads") of defendant's news articles on Facebook,

6. 3. under no circumstances does the defendant collect or process personal data of users. The only use of Facebook made by the defendant is to promote her news articles to more people on the basis of the criteria provided by the platform.

6.4. the defendant does not keep a record of the personal data of any user who visits the site from a Facebook link.

7. In a letter from my Office to the defendant dated 30 May 2022, it was stated inter alia that the use of the Facebook pixel tool results in the processing of data of users – visitors to the website. This data can lead to user-visitor identification, possibly in combination with other data. Therefore, the visit of internet users to the website results in the processing of their personal data, even if it was not the intention of the defendant. Therefore, the respondent was again requested to reply to the questions contained in the Office's letter of 20 January 2022.

8. However, the defendant did not provide any reply or information to my Office.

B. Legal framework

9. According to Article 4 of the Regulation, personal data are to be interpreted as *'any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one 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'*.

10. The controller is defined in Article 4 of the Regulation as *'the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law'*.

11. A processor is defined in Article 4 of the Regulation as *'*a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller*'.*

12. Regarding the principles governing the processing of personal data, Article 5 of the Regulation provides the following:

‘1. Personal data shall be:
(a) processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’);
(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (‘purpose limitation’);
(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);
(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’);
(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (‘storage limitation’);
(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’).’

13. Pursuant to Article 44 of the Regulation, it is provided that:

“Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.”

14. Pursuant to Article 57(1)(f) of the Regulation, the Commissioner for Personal Data Protection has the duty to:

“handle complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 80, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary.”

15. As regards the submission of a complaint to the Supervisory Authority, Article 77 of the Regulation provides that:

> *"Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation."*

16. Pursuant to Article 58(2) of the Regulation, the Commissioner for Personal Data Protection has the following corrective powers:

> *"a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;*
> *(b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;*
> *(c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;*
> *(d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;*
> *(e) to order the controller to communicate a personal data breach to the data subject;*
> *(f) to impose a temporary or definitive limitation including a ban on processing;*
> *(g) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19;*
> *(h) to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;*
> *(i) to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case;*
> *(j) to order the suspension of data flows to a recipient in a third country or to an international organisation.'*

17. As regards the general conditions for imposing administrative fines, Article 83(2) of the Regulation provides:

> *'2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:*
> *(a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;*
> *(b) the intentional or negligent character of the infringement;*

(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;
(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;
(e) any relevant previous infringements by the controller or processor;
(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;
(g) the categories of personal data affected by the infringement;
(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;
(i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;
(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and
(k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

3. If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.

4. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:
(a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;
(b) the obligations of the certification body pursuant to Articles 42 and 43;
(c) the obligations of the monitoring body pursuant to Article 41(4).

5. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:
(a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;
(b) the data subjects' rights pursuant to Articles 12 to 22;
(c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;
(d) any obligations pursuant to Member State law adopted under Chapter IX;
(e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).”

C. Rationale

18. On the basis of the information provided by the complainant, it appears that the subject of the complaint is the possible transfer of data by the complainant and whether there was an adequate level of data protection, as provided for in Article 44 of the Regulation, due to the inclusion of a Facebook tool on the website. In this context, it should also be investigated whether Facebook Ireland and/or Facebook Inc. have an obligation to comply with Article 44 of the Regulation.

19. At this point, I note that any further processing is not addressed in this Decision. I also note that I do not consider whether the transfer was made directly by defendant to Facebook Inc. or via Facebook Ireland. The question is whether, in the case of a transfer, there was the required level of protection of the data transmitted.

20. The defendant is a private news company. The defandant's website contains articles of a variety of topics, in Greek. Taking into account the themes of the website's content, it appears that the website is targeted at persons present in Cyprus. Furthermore, the defendant is based and active only in Cyprus and not in another Member State.

21. The Facebook Pixel tool (hereinafter the "tool") is a piece of code that is placed on a website and allows measuring the effectiveness of the company's website ads by understanding the actions that users take on the site. Based on information on a Facebook website, Meta's Pixel tool (as it's now called) can help the site-company understand the effectiveness of its ads and the actions users take on the site, such as visiting a page or adding a product to the cart. It is also possible for the company to see when customers have taken any action after seeing the ad on Facebook and Instagram, which can help with retargeting. The Facebook Pixel tool is used to make sure the company's ads are displayed to the right people, increase the company's sales, and measure the results of its ads.

22. Regarding the tool, a relevant Facebook website mentions the following:
The Meta Pixel can collect the following data:
— HTTP Headers – Anything that is generally present in HTTP headers, a standard web protocol sent between any browser request and any server on the internet. This information may include data like IP addresses, information about the web browser, page location, document, referrer and person using the website.
— Pixel-specific Data – Includes Pixel ID and the Facebook Cookie.
— Click Data – Includes any buttons clicked by site visitors, the labels of those buttons and any pages visited as a result of the button clicks.
— Optional Values – Developers and marketers can optionally choose to send additional information about the visit through Custom Data events. Example custom data events are conversion value, page type and more.
— Form Field Names – Includes website field names like email, address, quantity, etc., for when you purchase a product or service. We don't capture field values unless you include them as part of Advanced Matching or optional values.

23. It is not known when the tool was installed on the site. However, by studying the har file submitted by the complainant, it is confirmed that at the material time the tool was installed.

24. The defendant decided to integrate the tool into the website for purposes that it has defined. The defendant did not mention to my office the purpose for which she incorporated

the tool. However, in view of its reply that the Facebook pixel tool is a paid ads tool of the defendant's Facebook news articles, I consider that the purpose of the inclusion is included in the above reply. Therefore, because of its own choice decision, the tool code, which was provided to it by Facebook, was installed.

25. In the light of the above, I find that the defendant is the controller for that processing, after it has determined the purposes and means of the processing.

26. Due to its own decision to incorporate the tool, the complainant's personal data was processed. Even if no processing is carried out directly by the defendant or, as she herself mentioned, does not keep a record of the personal data of any user who visits the site, from a Facebook link, any processing is made due to the defendant's own decision to integrate the tool.

27. Therefore, as a controller, it had to take all measures so as not to undermine the level of protection of personal data which it processes or entrusts to a processor.

28. The Terms of Use of Facebook Business Tools, in section 5.a., state that:

To the extent that Business Tool Data includes Personal Data that you process in accordance with the General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR"), the following terms will apply:

I. The parties acknowledge and agree that you will have the role of Data Controller in relation to the processing of Personal Data included in the Business Tool Data for the purposes of providing the matching, measurement and analysis services described in paragraphs 2.a.i and 2.a.ii above (e.g. for the provision of Analysis and Reporting for Campaigns), and that you give to Facebook Ireland Ltd.; 4 Grand Canal Square, Grand Canal Harbour, Dublin 2 Ireland ("Facebook Ireland") to process on your behalf, and as a Data Processor, such Personal Data for these purposes, in accordance with the Terms of Use of the Business Tools and the Facebook Data Processing Terms. The Data Processing Terms are explicitly incorporated herein by reference and govern your relationship with Facebook Ireland in conjunction with the Terms of Use of the Business Tools.

II. With regard to Personal Data contained in Event Data, it concerns user actions on your websites and apps that incorporate Facebook Business Tools, and for the means and purposes of which you jointly decide with Facebook Ireland, you and Facebook Ireland acknowledge and agree that you will act as Data Controller jointly, in accordance with Article 26 of the GDPR. The joint responsibility for the processing of the data also extends to the collection of such Personal Data through Facebook Business Tools and its subsequent transmission to Facebook Ireland for use for the purposes specified in paragraphs 2.a.iii to 2.a.v.1 ("Joint Processing") above. For more information, click here. The Joint Processing is subject to the Annex for Data Controllers, which is expressly incorporated herein by reference and governs your relationship with Facebook Ireland in conjunction with the Terms of Use of the Business Tools. Facebook Ireland remains an independent Data Controller pursuant to Article 4(7) of the GDPR for the processing that takes place after the data has been transferred to Facebook Ireland.

III. You, as appropriate, and Facebook Ireland remain independent Data Controllers pursuant to Article 4(7) of the GDPR for the processing of Personal Data included in Tool

Data for businesses that, according to the GDPR, are not subject to paragraphs 5.a.i and 5.a.ii."

29. There is therefore an assumption by Facebook of the relationship it has with the defendant in relation to the processing of the personal data of visitors to the site. On the basis of this relationship, Facebook Ireland is entrusted with the processing of data by the controller. There are also cases where the defendant and Facebook Ireland have the role of joint controller. However, it is not stated in any way that the defendant has a role other than the above.

30. As mentioned by the complainant, on 12 August 2020 at 11:43 a.m., he visited the website while logged in to a Facebook account with his email address. The har file, which the complainant submitted to my Office, contains information on the communication between the web server and the complainant – visitor, as well as information on cookies used during navigation. Also, data sharing, through cookies, has been revealed from services provided by Facebook.

31. It also includes the cookie file _fbp, which is stored on the user's device – visitor to a website. With regard to this file, Facebook provides the following information on its website:
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 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'

32. The Facebook Data Processing Terms document states that:
Facebook, Inc. has made commitments under the EU-U.S. Privacy Shield and Swiss-U.S. Privacy Shield that may apply to data transferred by you or Facebook Ireland Limited to Facebook, Inc. under the Applicable Product Terms. This refers to a transfer of data from the EU/EEA either directly from the website – company or from Facebook Ireland.

33. Therefore, due to the application of the Facebook Pixel tool on the website, at least the IP address, browser information, website location, pixel ID and click data on the complainant's terminal were processed.

34. Because the tool is embedded in the website, Facebook has the technical ability to obtain the information that a particular Facebook account user has visited that website if the user is logged in to his Facebook account.

35. As a result of the application of the Facebook Business Tools tool on the website, cookies were placed on the complainant's terminal device, which contain a unique randomly generated price. This makes it possible to personalise the complainant's terminal device and record his/her navigation behaviour in order to display appropriate personalised advertising.

36. The defendant stated that under no circumstances does it collect or process personal data of users. However, even if it does not process it itself, this processing is carried out because of its own decision to integrate the tool into the website.

37. The European Data Protection Supervisor's decision of 5 January 2022 against the European Parliament on the use of Google Analytics states that cookies that make the user identifiable constitute personal data, regardless of whether the user's identity is unknown or deleted after its collection. It is also stated that all data containing identifiers that can be used to identify/segregate users are considered personal data and should be handled and protected as such. Although the European Data Protection Supervisor is responsible for the application of Regulation (EU) 2018/1725, this can also be interpreted in this case.

38. Guidelines 5/2021 of the European Data Protection Board on the interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the Regulation provide for the following three cumulative criteria for the qualification of a processing operation as a transfer:
"1) A controller or a processor ("exporter") is subject to the GDPR for the given processing.

2) The exporter discloses by transmission or otherwise makes personal data, subject to this processing, available to another controller, joint controller or processor ("importer").

3) The importer is in a third country, irrespective of whether or not this importer is subject to the GDPR for the given processing in accordance with Article 3, or is an international organisation."

39. In relation to the above, the following are apparent:
39.1. the defendant is established in Cyprus and is responsible for the operation of the website,
39.2. the defendant disclosed personal data of the complainant due to the installation of the tool on the website, which resulted in their (final) disclosure to Facebook Inc.,
39.3. Facebook Inc. has a registered office in the U.S.

40. Therefore, sharing data on Facebook Inc. is a data transfer.

41. Pursuant to Article 28(1) of the Regulation, the defendant, as a controller, is obliged to use only processors who provide sufficient assurances for the implementation of appropriate technical and organisational measures in such a way that the processing meets the requirements of the Regulation and ensures the protection of the data subject's rights. In the present case, after the defendant incorporated the tool, it implies that the defendant accepted the terms of data processing contained in the Facebook Business

Tools document and agreed that Facebook Inc. acts as a sub-processor. That document states, inter alia, that:
‘2. You agree that Facebook may subcontract its data processing obligations under these Terms of Use for data processing to a subprocessor. However, this can only be done by means of a written agreement with the subprocessor which imposes obligations on the subprocessor that are no less burdensome than those imposed on Facebook by these data processing terms. If a subprocessor fails to comply with such obligations, Facebook remains fully liable to you for the fulfilment of the obligations of this subprocessor. You currently authorise Facebook to oblige Facebook Inc. (and other Facebook companies) as its subprocessors. Facebook must inform you in advance of (any) any additional subprocessor(s).

42. On the basis of the information on a Facebook website on the EU-US Privacy Shield, the following is provided:
You acknowledge that the use of certain Facebook services for advertisements or measurements (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 referring to the EU-US Privacy Shield or the Swiss-US Privacy Shield (collectively, ‘Privacy Shield’). If the Privacy Shield applies to the data you provide and without limiting any agreement between you and Facebook, you acknowledge and agree to:
— Facebook’s Privacy Shield Notice is available at www.facebook.com/about/privacyshield; he explains the certification of Facebook. In accordance with your obligations in connection with your use of the Services, you undertake to provide persons with reasonable and appropriate information about the Services.
— Facebook may provide data subjects with contact information about you through the Services, allowing them, among other things, to contact you directly in order 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. However, you will remain responsible for resolving any complaints made to you by data subjects regarding your processing of the personal data subjects in connection with the Services (whether they are directly addressed to you or to us).
— You undertake to take all reasonable steps (including those reasonably requested by Facebook) to enable Facebook to comply with its Privacy Shield obligations, including assistance to resolve complaints. In the event of a conflict between these Terms of Use and other Terms of Use that invoke these Terms of Use, these Terms of shall Use Prevail.

Last change: September 29, 2017»

43. On the basis of the above, it appears that due to the visit to the website, data may be transferred to the United States. However, the defendant does not acknowledge at all the possibility of transmission, nor has it answered the relevant questions put to it. Furthermore, it has not provided me with any evidence that no data transmission took place.

44. Furthermore, it appears that at the material time, data transfers made due to the visit to the website were based on the EU-US Privacy Shield.

45. Facebook Inc. is classified as a provider of electronic communications services within the meaning of 50 U.S. Code § 1881(b)(4) and is therefore subject to oversight by

U.S. intelligence services in accordance with 50 U.S. Code § 1881a ("FISA 702"), and is therefore obliged to provide U.S. authorities with personal data.

46. Due to the transfer to the United States of America, access to the complainant's personal data could be made by the U.S. authorities, which the defendant cannot ascertain. In this case, the defendant is not relieved of its responsibility for the protection of the complainant's personal data. Moreover, the defendant continued to maintain the tool on its website, even after the judgment of the European Court of Justice, Case C-311/18, dated 16 July 2020, declaring the 'EU-US Privacy Shield' invalid (Commission Implementing Decision (EU) 2016/1250 of 12 July 2016).

47. In the case of transmission, the relevant obligations set out in Chapter V of the Regulation should be complied with. In particular, an adequate level of protection of the data transferred should be provided, as provided for in Article 44 of the Regulation. Therefore, one of the following conditions should be met:
47.1. an adequacy decision pursuant to Article 45 of the Regulation,
47.2. appropriate safeguards, pursuant to Article 46 of the Rules of Procedure,
47.3. derogations for specific situations under Rule 49 of the Rules of Procedure.

48. Due to the above ruling of the European Court of Justice, Case C-311/18, there was no U.S. adequacy decision at the material time.

49. This Decision does not require a more detailed analysis of the legal situation of the United States (as a third country), since the CJEU has already dealt with it in its abovementioned judgment of 16 July 2020. Based on the CJEU ruling, it appears that the EU-US adequacy decision did not provide an adequate level of protection for individuals under the relevant U.S. legislation and the implementation of official surveillance programmes, including under section 702 FISA and Executive Order 12333 in conjunction with Presidential Policy Directive 28 (PPD-28).

50. Furthermore, the defendant has not informed my Office of the existence of appropriate safeguards under Article 46 of the Regulation or of derogations for specific situations under Article 49 of the Regulation. In any event, one of the derogations provided for in Rule 49 of the Rules of Procedure cannot be invoked as a legal basis.

51. On the basis of all the foregoing, I therefore find that the defendant has not shown that, as a result of the transfer, the level of protection of natural persons guaranteed by the Regulation is not undermined, contrary to Article 44 of the Regulation.

52. Pursuant to Article 5(2) of the Regulation, the controller is responsible and is able to demonstrate compliance with paragraph 1 ('accountability'). However, on the basis of the positions submitted by the defendant to my Office, I note that it has not only failed to demonstrate compliance with Article 5(1) of the Regulation, but also does not recognise the processing carried out as a result of its own decision to incorporate the tool.

53. I therefore find that Article 5(2) has been infringed by the defendant. This would be the case even if the complainant's data were not transferred to the United States.

54. The complainant also requested that it be clarified whether the provisions of the Facebook Business Tools Terms and Facebook Data Processing Terms, at the time of

lodging the complaint and as to be amended as of 31 August 2020, met the requirements of Article 28 of the Regulation on the transfer of personal data to third countries.

55. According to Article 5 of the Regulation, the controller is responsible for complying with the principles governing the processing of personal data. However, the possibility that Facebook Inc. will receive requests from U.S. security authorities does not automatically lead to the conclusion that it has determined the purposes and means of the processing, i.e. that it is considered a controller under Article 28(10) of the Regulation. Nor can Facebook Ireland or Facebook Inc. be held liable for a breach of Article 28, since, under that article, the controller bears such responsibility.

56. In addition to the above, it will be necessary to examine whether Facebook Inc. is, in the present case, subject to the obligations set out in Chapter V of the Regulation. On the basis of Guidelines 5/2021 of the European Data Protection Board, a transfer exists where "The exporter communicates by means of a transfer or otherwise makes available personal data, which are subject to such processing, to another controller, joint controller or processor ('importer')". Therefore, the requirements of Chapter V of the Regulation must be complied with by the data exporter, i.e. the defendant, but not the data importer, in this case Facebook Inc.

57. Therefore, in assessing this transfer, no breach of Article 44 of the Regulation by Facebook Inc. can be established.

D. Conclusion

58. In the light of all the above elements, as set out above, and in the light of the powers conferred on me under Article 57(1)(f) of the Regulation, I find that there has been a breach by the defendant:
58.1. Article 5(2) of Regulation (EU) 2016/679, by failing to demonstrate compliance with Article 5(1) of the Regulation, i.e. the principle of accountability; and
58.2. Article 44 of Regulation (EU) 2016/679, because it did not ensure that the level of protection of the reporting person guaranteed by the Regulation is not undermined.

59. After taking into account and taking into account:

(a) the legal basis in force concerning the administrative penalties provided for in Article 58(2) and Article 83 of the Regulation,

(B) all the circumstances and factors which the complainant and the defendant brought before me on the basis of all existing correspondence,

I consider that, in the circumstances, the imposition of an administrative fine is not justified.

Also, in view of the new EU-US Data Protection Framework, Commission Implementing Decision (EU) 2023/1795 of 10 July 2023 on the adequacy of the level of protection of personal data under the EU-US Data Protection Framework, I consider that it is not justified to impose an immediate prohibition or suspension of any transfer of data by Defendant to Facebook Inc.

60. Nevertheless, having regard to the above facts, the legal aspect on which this Decision is based and the analysis as explained above, and exercising the powers conferred on me by Article 58(2)(b) of the Regulation,

I decided

in my opinion and in compliance with the above provisions, I should address to the ARKTInos Publications Ltd (“Politis” newspaper):

Reprimand for the violation of Article 5(2) of Regulation (EU) 2016/679;
Reprimand for the violation of Article 44 of Regulation (EU) 2016/679, and
Order to ensure that, if it continues to use the tool, the transfer can take place on the basis of the new EU-US Data Protection Framework, Implementing Decision (EU) 2023/1795, or on the basis of an appropriate guarantee under Article 46 of the Regulation,and inform me thereof within one month of receipt of this Decision.

Irene Loizidou Nicolaidou
Commissioner for
Personal Data Protection

28 February 2024