REPUBLIC OF CYPRUS

OFFICE OF THE COMMISSIONER
FOR PERSONAL DATA PROTECTION

MACHINE TRANSLATED

Case Reg.: 11.17.001.008.227

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 the Cyprus Football Association (hereinafter the "defendant"), as well as against Google LLC. 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 visited the website http://cfa.com.cy (hereinafter the "website") on 14 August 2020 at 10:41 a.m. while logged in to a Google account with his e-mail address,

2.2. the defendant has integrated HTML code for Google Services (including Google Analytics),

2.3. during the complainant's visit to the website, the defendant processed his personal data (at least the IP address and cookie data), at least some of which were transmitted to Google;

2.4. the use of Google Analytics is subject to the Google Analytics Terms of Service and the Google Ads Data Processing Terms, which have been updated with effect from August 12, 2020 (Google Ads's New Data Processing Terms);

2.5. under the Google Analytics Terms of Service, Google LLC (1600 Amphitheatre Parkway Mountain View, CA 94043, USA) is the controller's contracting partner. In

accordance with point 5.1.1(b) of the Google Ads Data Processing Terms and the New Data Processing Terms of Google Ads, Google LLC processes personal data on behalf of the controller and fulfils the conditions as a data processor in accordance with Article 4(8) of the Regulation,

2.6. according to point 10 of the Google Ads Data Processing Terms, the controller has agreed that Google may store and process personal data (in this case of the complainant) "[...] in the USA or any other country in which Google or any of its Subprocessors maintain facilities". Such transfer of the complainant's personal data from the controller (EEA-based company) to Google LLC or its subordinates in the U.S. (or any other country outside the EEA) requires a legal basis under Article 44 and subsequent articles of the Regulation;

2.7. as the CJEU has annulled the EU-US Privacy Shield decision in judgment C-311/18, the controller can no longer base the transfer of data to Google LLC in the U.S. on an adequacy decision under Article 45 of the Regulation. However, the controller and Google LLC continued to rely on the invalidated "EU-US Privacy Shield" for almost four weeks after the decision, as evidenced by point 10.2. of the Google Ads Data Processing Terms.

2.8. 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;

2.9. Google LLC fulfils the conditions 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 shown by the Snowden Slides and Google LLC Transparency Report (https://transparencyreport.google.com/userdata/us-national-security), Google LLC actively provides personal data to the U.S. Government pursuant to 50 U.S. Code § 1881a;

2.10. consequently, the controller is unable to ensure adequate protection of the complainant's personal data transferred to Google LLC. However, since 12 August 2020, the controller and Google LLC have tried to rely on standard contractual clauses for data transfer to the U.S., as evidenced by point 10.2. of Google Ads's New Data Processing Terms.

2.11. this practice completely ignores paragraphs 134 and 135 of the above CJEU judgment, which imposes a legal obligation on the controller to refrain from transferring the data of the complainant, or others, to Google LLC in the U.S. However, for more than one month after the decision, the controller has not acted on the basis of the judgment;

2.12. similarly, Google LLC continues to accept data transfers from the EU/EEA, on the basis of standard contractual clauses, despite the clear judgement of the CJEU and in violation of Articles 44 to 49 of the Regulation. Google LLC further discloses personal data from the EU/EEA to the U.S. government in violation of Article 48 of the Regulation. In many public statements, Google has acknowledged that it has not changed this practice:

The Privacy Shield frameworks provided a mechanism to comply with data protection requirements when transferring EEA, UK or Swiss personal data to the United States and onwards. While the Swiss-U.S. Privacy Shield currently remains valid, in light of the recent Court of Justice of the European Union ruling on data transfers, invalidating the EU-U.S. Privacy Shield, Google will be moving to depend on Standard Contractual Clauses for relevant data transfers, which, as per the ruling, can continue to be a valid legal mechanism to transfer data under the GDPR. We are committed to having a lawful basis for data transfers in compliance with applicable data protection laws.'

2.13. 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, namely Google LLC,

2.14. 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;

2.15. the complainant requests that:
2.15.1. the complaint under Article 58(1) of the Regulation has been fully investigated and clarified:
(a) what personal data has been transferred by the defendant to Google LLC in the U.S. or any other third country or international organisation;
(b) on which transmission mechanism the respondent based the transfer of data;
(c) whether the provisions of the Google Analytics Terms of Service and the (New) Data Processing Terms of Google Ads, when submitting the complaint, met the requirements of Article 28 of the Regulation regarding the transfer of personal data to third countries;

2.15.2.immediately prohibit or suspend any transfer of data from the defendant to Google LLC in the U.S., and order the return of the data to the EU/EEA or another country providing adequate protection pursuant to Article 58(2)(d), (f) and (j) of the Regulation;

2.15.3.an effective, proportionate and dissuasive fine shall be imposed against the defendant and Google LLC, 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 (Article 83(2)(a) of the Regulation);
(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 letters to the defendant with clarification questions, on 23 December 2020 and 10 June 2022.

4. In letters dated 29 January 2021 and 13 July 2022, the defendant stated, inter alia, that:

4.1. in order to comply with the 2004 Law on the Regulation of Electronic Communications and Postal Services (Law 112(1)/2004) and the Regulation, the defendant instructed legal advisers and other consultants to advise it in order to establish and implement relevant compliance policies, including the necessary forms or tools. Among the advice was the posting of a specialised and up-to-date user consent tool ("cookie banner"). However, inadvertently there was a delay in posting the mentioned cookie banner which has already been done and the cookie banner is now posted on the website, while it is mentioned in the Cookie Policy of the defendant,

4.2. the website uses cookies as described in the Cookie Policy posted on it, including analytical Google Analytics cookies;

4.3. consent to the use of analytical data: according to Article 99(5) of Law112(I)/2004, analytical cookies are not strictly necessary cookies since their sole purpose is not to "carry out the transmission of a communication, over an electronic communications network", nor are they "absolutely necessary to enable the provider of an information society service explicitly requested by the subscriber or user to provide the service in question".

4.4. personal data:
4.4.1. recital 30 of the Regulation states: "Natural persons may be linked to online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. These may leave traces which, in particular when combined with unique identifiers and other information received by servers, can be used to create the profile of natural persons and identify them."

4.4.2. Google Analytics collects various data (data) such as: pages visited by the user and time spent on each page, site detail reference (such as URL), browser type, operating system type, IP address, etc. The defendant is unable to identify the user only from the use of this data due to the absence of a combination with other identifiers that leave traces and thus allow the identification of the user. This is also explained by the purely informative nature of the defendant's website. In other words, the user does not submit personal data since he is not required to have an account to use the website (login), nor is there any possibility of buying products and services (shopping basket), nor is there any other way of verifying his identity when browsing the website (authentication);

4.4.3. despite the above, the defendant understands that by storing such data, as a result of the use of cookies, there is even a minimum likelihood of the user being indirectly identified if combined with other identifiers. For such processing of personal data, the user gives his or her consent through the relevant tool posted on the website;

4.5. transfer of personal data to a third country outside the EEA, pursuant to Chapter V of the Regulation:
4.5.1 some of the data collected from the use of analytical cookies (e.g. IP address) may be transmitted to Google servers located in the United Kingdom or the United States;

4.5.2. in its recent judgment C-311/18 (Schrems II – July 2020), the Court of Justice of the European Union (CJEU) declared the Privacy Shield decision invalid. At the same time, the CJEU considered that the lawfulness of the transfer of personal data on the basis of the standard contractual clauses should be determined by the outcome of the evaluation

of the data and the circumstances of the transfer, as well as the additional measures that could be implemented,

4.5.3. on this basis, the European Data Protection Board with Recommendations 01/2020 announced a roadmap on the steps (5 steps) to be followed by data exporters in order to determine whether they need to take additional measures to be able to lawfully transfer data outside the EEA. Reference is made to steps 2, 3 and 4 regarding possible data transfers to Google's U.S. server:
4.5.3.1. step 2 and 3: verification of the transmission tool on which the transfer is based and evaluation of legislation of the third country, which could affect the effectiveness of the transmission tools on which the exporter relies:
Google claims that it continues to rely on standard contractual clauses. It has also announced that it has renewed the terms of use of its services (e.g. Google Analytics) to appear to be based on the new standard contractual clauses. Google announced in August 2020 that "we will continue to monitor the evolution of data transfer mechanisms under the GDPR and are committed to having a legal basis for data transfer in accordance with applicable data protection laws."

Considering that: a) the U.S. has not been recognised by the EU as a country with an adequate level of protection of personal data, and b) in Schrems II the CJEU found that transfers to companies such as Google that are subject to "FISA 702" violate the protection principles of the Regulation, the defendant decided that although Google still relies on standard contractual clauses, it would be safe and feasible to rely "in addition" on the basis of Article 49(1)(a) of the Regulation, i.e. on the explicit consent of the user. In this way, it is understood to the user, through the Cookie Policy and the cookie banner, that the data may be transferred to the U.S. under conditions and taking additional protection measures, as described below (step 4). The defendant does not overlook the fact that there was a delay, by mistake, in the posting of the cookie banner, but the defendant's Policy and its mode of operation are in line with the spirit of Article 49(1)(a) of the Regulation;

4.5.3.2. step 4: additional measures:
taking into account the above, the defendant set these cookies in such a way that the IP address of the user/visitor is stored and transmitted after anonymisation of the IP address (Annex 2 of Recommendations 01/2020). Anonymisation/mask of IP addresses takes place immediately after data is received from the Google Analytics collection network, prior to storage or processing;

4.6. recipients of cookies:
apart from the cookie service providers (e.g. Google), the cookie data is not transferred to other third parties without the knowledge of Provence, except where such providers use third parties to enable the provision of their services, where it is legally permissible to do so or where the providers transfer or transfer data to third parties as a result of their direct relationship with users. The defendant also uses the developers of the website who, among other things, are responsible for the technical settings of cookies on the website;

4.7. duration of treatment:
the defendant will process information as a result of the use of cookies for as long as the cookies last as shown in the Cookie Policy and in the banner cookies;

4.8. the defendant believes that it has taken into account the relevant legislation governing the use of cookies and the protection of personal data, and has adopted all

reasonably necessary technical measures for the protection of the user's data, as well as transparency measures regarding the detailed information to the user on the use of cookies by the defendant;

4.9. the defendant has developed and established transparent accountability mechanisms and makes a serious and continuous effort to improve its compliance with the Regulation, always respecting the rights and freedoms of those who visit the website, as well as the interests of stakeholders and those who expect it, and is willing to cooperate fully with my Office on the above;

4.10. following my request for a signed copy of the standard contractual clauses to be submitted to my Office, clearly showing the standard clauses used and the role of the defendant, the defendant submitted a Google website address containing the standard contractual clauses in force at the time.

However, the defendant has not answered my Office's questions relating to standard contractual clauses, such as:
4.10.1. if it has verified (with the addressees) that there is nothing in the law of the third country prohibiting recipients from complying with their contractual obligations as resulting from the standard contractual clauses, with a view to ensuring that the level of data protection of individuals guaranteed by the Regulation in the EEA is not undermined;

4.10.2.if it has concluded that the addressees can effectively guarantee the fulfilment of their contractual obligations as set out in the standard contractual clauses, what were the detailed reasons for such termination by providing appropriate evidence;

4.10.3.if it has concluded that the addressees cannot guarantee the fulfilment of their contractual obligations as set out in the standard contractual clauses, whether it has considered the application of additional measures, and if so, which ones. Furthermore, it has verified that these additional measures can be implemented in practice and that there is nothing in the legislation of the third country that prevents recipients from doing so, in order to ensure that the level of data protection of individuals guaranteed by the Regulation in the EEA is not undermined. What was, in detail, the result of this assessment and what were the reasons for the outcome of the defendant?

4.11. the defendant submitted to my Office:
4.11.1.a copy of the record of processing activities;
4.11.2.a copy of the Cookie Policy; and
4.11.3.screenshot showing the existing cookie banner settings.

In the record of processing activities is included a "Website Data" processing activity, with the following information:
— legal basis: consent,
— purpose: use of cookies on the website for the sole purpose of personalising content, for the provision of functional means and for the analysis of browsing on our website;
— data subjects: users/visitors of the website,
— personal data: IP address, MAC address, cookies etc,
— categories of recipients: website administrators/supporters and cookie service providers (e.g. google);
— data transmission: yes to cookie providers (e.g. google) based on standard contractual clauses and/or Article 49(1)(a) of GDPR 2016/679;

— envisaged period: for the duration of cookies in each case.

B. Legal framework

5. 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'.*

6. 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'.*

7. 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*'.*

8. 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').'

9. 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."

10. 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."

11. 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."

12. 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.'

13. 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

14. 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 integration of the Google Analytics tool (hereinafter the “tool”) on the website. In this context, it should also be investigated whether Google LLC has an obligation to comply with Article 44 of the Regulation.

15. At this point, I note that any further processing is not addressed in this Decision.

16. The defendant is a legal person. Among its objectives is the organisation and supervision of Cypriot football and its representation in international football. The defendant provides information on its website on Cypriot football, in Greek and English. 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.

17. Google Analytics is a measurement service that allows website owners to measure, among other things, traffic characteristics. This includes measuring the traffic of visitors visiting a particular website. This enables an understanding of the behaviour of website visitors and how they interact with a particular website. In particular, a website owner can create a Google Analytics account and display reports about the site using a dashboard. Google Analytics can also measure and optimise the effectiveness of website owners’ advertising campaigns on Google ad services.

18. 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.

19. The defendant decided to integrate the tool into the website http://cfa.com.cy, for the sole purpose, as stated in the activity file, “to personalise content, to provide functional means and to analyse the browsing of our website”. Therefore, because of its own choice decision, the tool code, which was provided to it by Google LLC, was installed.

20. On the basis of the above decision of the defendant, I find that the defendant is the controller for the specific processing, after it has determined the purposes and means of the processing.

21. 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, any processing carried out has arisen as a result of the decision of the defendant itself.

22. 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.

23. Point 5.1.1(b) of the Google Ads Data Processing Terms (date 1 January 2020) and the Google Ads New Data Processing Terms (date 12 August 2020) states:
‘(b) Google is a processor of Customer Personal Data under the European Data Protection Legislation;’

24. Point 10 of the Google Ads Data Processing Terms (date 1 January 2020) states that:
Data Storage and Processing Facilities. Customer agrees that Google may, subject to Section 10.2 (Transfers of Data), store and process Customer Personal Data in the United States of America and any other country in which Google or any of its Subprocessors maintain facilities.

24.1. Also, point 10 of the New Data Processing Terms of Google Ads (date 12 August 2020) states that:
Data Storage and Processing Facilities. Customer agrees that Google may, subject to Section 10.2 (Transfers of Data), store and process Customer Personal Data in any country in which Google or any of its Subprocessors maintain facilities.

25. There is, therefore, an assumption by Google LLC of its relationship with the defendant in relation to the processing of the personal data of visitors to the website. On the basis of this relationship, Google LLC is entrusted with the processing of data, on behalf of the controller, which may take place in any country that Google LLC or its sub-executors have facilities.

26. Moreover, in its letter of 29 January 2021, the defendant refers to Google as ‘the Google processor’.

27. As mentioned by the complainant, on 14 August 2020, at 10:41 a.m., he visited the website while logged in to a Google 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. In addition, data has been disclosed, through cookies, from services provided by Google for marketing and analytics purposes.

28. It also includes the _ga and _gid cookies, which are stored on the user's device – visitor to a website. In these cookies, unique user identification numbers are processed. Unique numbers make it possible to distinguish between visitors to a website and whether or not visitors have visited the site in the past. By using only these identification numbers, it is possible to distinguish visitors to a website.

29. On the basis of the above, it appears that the complainant's personal data has been processed. Its unique user identification numbers and IP address were processed, including transmission.

30. Besides, there is an assumption from the defendant that Google Analytics collects various data (evidences) such as: pages visited by the user and time spent on each page, site detail reference (such as URL), browser type, operating system type, IP address, etc.

31. The defendant stated that it is unable to identify the user only from the use of this data due to the absence of a combination with other identifiers that leave traces and thus allow the user to be identified. It also stated that this is also explained by the purely informative nature of the website, i.e. the user does not submit personal data since he is not required to have an account to use the website (login), nor is there any possibility of buying products and services (shopping basket), nor is there any other way of verifying his identity when browsing the website (authentication). However, the above positions of the defendant do not call into question the relevant data processing carried out.

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

33. 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.

34. According to the case law of the ECJ, in particular on the basis of the judgment of the Court of Justice of 17 June 2021, C-597/19, and the judgment of the Court of Justice of 19 October 2016, C-582/14, it appears that the IP address is a personal data, pursuant to Article 4 of the Regulation. The IP address also does not lose its status as a personal data because the means of identification belong to third parties.

35. Combining unique user identification numbers with other elements, such as browser data or IP address, may lead to user identification. It follows that the complainant could be identified as a result of the inclusion of the tool on the website. Moreover, the defendant has indicated to my Office that it understands that by storing specific data, as a result of the use of cookies, there is even a minimum likelihood of the user being indirectly identified, if combined with other identifiers.

36. 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."

37. In relation to the above, the following are apparent:
37.1. the defendant is established in Cyprus and is responsible for the operation of the website,
37.2. the defendant disclosed personal data of the complainant due to the installation of the tool on the website, which resulted in their disclosure to Google LLC in the U.S.
37.3. Google LLC has a registered office in the U.S.

38. It follows that the installation of the tool on the website resulted in the complainant's data being transferred to the United States. At this point, I note that the defendant stated that some of the data collected from the use of analytical cookies (e.g. an IP address) may be transferred to Google's servers located in the United Kingdom or the United States.

39. Google LLC is designated 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.

40. 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).

41. In the case of transfer, 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:
41.1. an adequacy decision pursuant to Article 45 of the Regulation,
41.2. appropriate safeguards, pursuant to Article 46 of the Regulation,
41.3. derogations for specific situations under Article 49 of the Regulation.

42. 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.

43. 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).

44. On the basis of the information submitted to me, it appears that, at the material time, between defendant and Google LLC, standard contractual clauses were in force pursuant to Article 46(2)(c) of the Regulation. In the above CJEU judgment of 16 July 2020, it was stated that standard contractual clauses, as a transmission tool, cannot bind the authorities of the third countries. In particular, it is stated that:
" 125. However, although those clauses are binding on a controller established in the European Union and the recipient of the transfer of personal data established in a third country where they have concluded a contract incorporating those clauses, it is common ground that those clauses are not capable of binding the authorities of that third country, since they are not party to the contract.

126. Therefore, although there are situations in which, depending on the law and practices in force in the third country concerned, the recipient of such a transfer is in a position to guarantee the necessary protection of the data solely on the basis of standard data protection clauses, there are others in which the content of those standard clauses might not constitute a sufficient means of ensuring, in practice, the effective protection of personal data transferred to the third country concerned. That is the case, in particular, where the law of that third country allows its public authorities to interfere with the rights of the data subjects to which that data relates.'

45. The CJEU therefore concluded in its judgment that standard contractual clauses cannot provide, in order to comply with the level of protection required by EU law, guarantees which go beyond the contractual obligation. In particular, the Decision explains that:
'133. It follows that the standard data protection clauses adopted by the Commission on the basis of Article 46(2)(c) of the GDPR are solely intended to provide contractual guarantees that apply uniformly in all third countries to controllers and processors established in the European Union and, consequently, independently of the level of protection guaranteed in each third country. In so far as those standard data protection clauses cannot, having regard to their very nature, provide guarantees beyond a contractual obligation to ensure compliance with the level of protection required under EU law, they may require, depending on the prevailing position in a particular third country, the adoption of supplementary measures by the controller in order to ensure compliance with that level of protection'.

46. In view of the above, and taking into account that the defendant did not refer to my Office any additional measures which were, in conjunction with the standard contractual clauses, in force at the material time, the above clauses cannot be regarded as an appropriate guarantee of transmission.

47. The defendant indicated to my Office that it would be safe and feasible to rely "in addition" on the derogation of Article 49(1)(a) of the Regulation, i.e. the explicit consent of the user – visitor.

48. However, the derogations for specific situations under Article 49 of the Regulation can only be used in individual situations and cannot be the rule. Therefore, user consent cannot be used for routine repetitive transmissions (such as the one triggered in each case when the user visits the website), but only as a derogation for special cases.

49. Therefore, the transmission of data cannot be based on Article 49(1)(a) of the Regulation and, more generally, on any other derogation as defined in that Article.

50. The defendant stated that it configured these cookies in such a way that the IP address of the user/visitor is stored and transmitted after anonymisation of the IP address. As he mentioned, the anonymisation/mask of IP addresses takes place immediately after data is received from the Google Analytics collection network, prior to storage or processing.

51. However, anonymisation of the IP address cannot be considered effective, since the data is processed by Google LLC prior to anonymisation. Even if it is considered that the IP address was processed only on servers in the EEA, it should be noted that under the relevant U.S. law, Google LLC may be required by U.S. intelligence services to provide the IP address. Moreover, the IP address is one of the various elements of the complainant's digital footprint, and not the only one.

52. It cannot be assumed that the anonymisation mentioned by the defendant ensures the appropriate level of security of the data of users – visitors to the website.

53. 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.

54. The defendant stated that by mistake there was a delay in posting a specialised and up-to-date consent tool for website visitors (cookie banner). Therefore, the existence of a cookie banner is intended for two reasons: a. informing users – visitors about the processing carried out, and b. obtaining consent for the processing.

This does not, of course, mean that the information makes the collection, storage and/or transmission of data legitimate, or that consent is the correct legal basis for such processing.

54.1. Moreover, it follows that at the material time, that is to say, when the complainant visited the website, the cookie banner was not integrated.

55. In addition to the above, it will be necessary to examine whether Google LLC 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 discloses by transmission or otherwise makes personal data, subject to this processing, available 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 Google LLC.

56. Therefore, in assessing this transfer, no breach of Article 44 of the Regulation can be established by Google LLC.

D. Conclusion

57. 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:
— Article 44 of Regulation (EU) 2016/679, because it did not ensure that the level of protection of the complainant guaranteed by the Regulation is not undermined.

58. 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 immediately, as requested by the complainant, a prohibition or suspension of any transfer of data from the defendant to Google LLC in the U.S.

59. 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 address to the Cyprus Football Association:

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