ROMÂNIA
AUTORITATEA NAŢIONALĂ DE SUPRAVEGHERE
A PRELUCRĂRII DATELOR CU CARACTER PERSONAL

Bld. Gen. Gheorghe Magheru Nr. 28-30, Sector 1, Cod poştal 010336, Bucureşti ; Tel. +40.31.805.9211; Fax:+40.31.805.9602 www.dataprotection.ro; e-mail: anspdcp@dataprotection.ro

ANSPDCP.Registrul Evidenta Decizii Avize Recomandari.0000068.08-10-2020

Decision

following the investigation performed Microstockr SRL

Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP), having the premises at 28-30 Gen. Gheorghe Magheru Blvd., 1st District, PO 010336, Bucharest, legally represented by [redacted], President issues this decision against [redacted], with its headquarters in [redacted], registered at the Trade Register under [redacted], fiscal identification code [redacted], represented by Mr. [redacted]

Considering the following:

I. PREMISE

1. Intimation pursuant to Article 56 of GDPR

By the application no. 66211/2019 introduced in IMI pursuant to Article 56 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation – hereinafter "GDPR"), the data protection authority from the Nordrhein-Westfalen Land (Germany) requested the opinion of ANSPDCP which it considers to be the lead authority (as the only office of the complained data controller is based on the Romanian territory) in the following case:

Mr. [redacted] (according to the annexes sent to the request[redacted]) complained that the right of erasure of his data related to an account created for the use of an application made available by [redacted] (based in [redacted]) was not respected. From the response sent by the controller including to the German authority, it is noted that the data and the account of the petitioner were initially deleted (after the free of charge use for one month of the application, for verifying its functionality), but subsequently he created a new account based on the same credentials and used the app again for a month free of charge. Against this situation, the controller decided not to delete his data in order to prevent the creation of a new account and the re-use of the application free of charge. [redacted] provides an application for photographers [redacted].

The German authority considers that many EU users use this application and, as such, the issue of data deletion seems to be a problem with cross-border impact.

Following the initiation of the procedure in IMI, the authorities from France, Denmark and Spain declared themselves to be concerned authorities as the processing would affect or could substantially affect data subjects in their country.

2. Responses of other supervisory authorities in IMI

A. Within the notification pursuant to Article 56 in IMI under no. 66211 (opened on the 6th of May 2019), the authorities from France, Denmark, Spain and Nordrhein-Westfalen Land of Germany declared to be concerned supervisory authorities.

Following the acceptance of the proposal to be the lead authority in this case, ANSPDCP opened the case of informal consultation in IMI under no. 71416, on the 9th of July 2019, pursuant to Article 60, specifying that the Romanian authority initiated an investigation and asking the other EU authorities for relevant information, if they consider themselves to be concerned supervisory authorities, with further explanations (e.g. how many complaints against [redacted] were received, on what subject etc.). In this case from IMI, the authorities of the following stated declared to be concerned authorities: Germany, Nordrhein-Westfalen Land (received one complaint), Czech Republic, France, Denmark, Sweden, Spain. The authorities from France and Denmark further explained that they noticed that there is a [redacted] mobile app in the Google Play Store and in App Store in French and English, explanation also given by the authorities from Sweden and Spain. Apart from the German authority, no other authority has stated that it had received any complaint against [redacted].

B. Following the introduction of a first draft of the decision issued by ANSPDCP in IMI (Article 60 118884), the authorities from France, Denmark, Spain (comments made in IMI) and Land of North Rhine-Westphalia (comments sent by e-mail) sent a series of comments on the legal basis chosen by the controller for not to delete the personal data in order to prevent fraud, on the method for obtaining the prior consent on the use of cookies, on prior information on the purposes of the processing, on the use of MD5 hash method that presents the risk of re-identification of the data subjects, on the data that are subject to the MD5 hash procedure, on the destination of the inactive accounts.

3. Investigation at [redacted]

ANSPDCP sent two investigation letters to [redacted]: letter no. 15899 of the 9th of July 2019; letter no. 21475 of the 24th of September 2019 (sent by regular mail and by electronic mail).

[redacted] replied to the two letters with: letter no. 20452 of the 10th of September 2019 (received through the court executor) and no. 20666 of the 12th of September 2019 (by electronic mail); letter no. 22258 of the 7th of October 2019 (sent by electronic mail) and no. 22297 of the 7th of October 2019 (sent by regular mail).

In order to clarify the issues raised by the authorities from France, Denmark, Spain and the Land of North Rhine-Westphalia, ANSPDCP sent the letter registered under no. 11372 of the 28th of May 2020, to which [redacted] responded with the letter registered under no. 11954 of the 9th of June 2020.

4. Minutes of the finding

Following the investigation, the minutes of the finding no. 17062 of the 24th of August 2020 was concluded, in which the following conclusions were held:

1. [redacted] application [redacted] in this way, it saves the user time and gives him/her an overview of his/her own portfolio;

2. when creating a new account, the following user data is collected: first name, last name, email and password of the [redacted] account. When the same user becomes a subscriber, the address, city, country, postal code and VAT code for invoicing are additionally collected (the VAT code is optional and is collected only in case of companies); this information is stored on the server, in the database of [redacted];
3. the representative of [redacted] stated that it processes the personal data of some persons (555 active clients) from 75 states (including all the EU states), thus fulfilling the conditions of cross-border data processing within the meaning of Article 4 point 23 letter b) of Regulation (EU) 679/2016 ("or processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State");
4. the personal data corresponding to each account are kept legible as long as the accounts are active; in case of deleted accounts, the personal data is kept in encrypted form during the existence of the application on the market, after which they will be deleted. An account is considered inactive after a period of 3 years form the last use. In the case of deleted accounts, the personal data is anonymised by using the hash functions by the MD5 encryption method;
5. currently, "the [redacted] accounts are deleted by contacting [redacted] and, after the request, the deletion operation is performed manually. This applied to all accounts, both those in the trial period and those with a subscription." The representative of [redacted] said that in the near future is planned to add a "Delete Account" button within the application that will allow the deletion automatically. When an account is deleted, the client's personal data are stored in encrypted form in the database, as a hash generated by MD5 encryption method. This data can no longer be decrypted and the person can no longer be identified. "A hash is from an account that has the trial period attached. When a user creates a new account with the same email, the hash of the new email is compared to each deleted account hash and, if they are identical, the deleted account is reactivated, overwriting the hashes with the data entered by the user, without benefiting once more of the free of charge month. The representative of [redacted] said that keeping there personal data in the hash form is the mechanism by which the controller is protected form the exploitation of the trial period. If the hashes do not match, a new account is created that will benefit from a "free trial" (one month trial period);
6. according to the statements of the representative of [redacted], the case of Mr. [redacted] (Germany) was an unique one in terms of exercising the right to erasure of data. The data collected in his case were first name, last name, [redacted] email account and [redacted] password. The account was initially created between 27 January and 27 February 2018 (the exact date is not know, the information being subsequently deleted). Following the request of the 25th of March 2018 to delete the account, Mr. [redacted] account was marked as deleted, but his data was kept to prevent fraud. On the 4th of April 2018 an email conversation with Mr. [redacted] takes place informing him that the email address and the agency account associated with the [redacted] as a measure to prevent the attempts to create again a new account free of charge. On the 27th of May 2018, Mr. [redacted], invoking the right to erasure of data provided by GDPR, requests the deletion of all [redacted] accounts associated with [redacted]. To this request, [redacted] responds on the 28th of May 2018 that it has deleted all personal data and saved the usernames associated to his account as hash MD5 in order to prevent the creation of a new free account. On the 30th of May 2018, Mr. [redacted] creates a new free account, used until the 30th of June 2018, a possible operation since at that time [redacted] had not yet implemented (for logistical reasons) the mechanism for verifying the creation of new accounts based on the dame data. On the 1st of July 2018, Mr. [redacted] requests the deletion of the data associated with the account [redacted], a request repeated on the 16th of July 2018. [redacted] informs the petitioner on the 2nd of July 2018 and on the 26th of July 2018 that it refuses to "erase the data". Mr. [redacted] again request information regarding the erasure of his accounts on the 15th of February 2019 and [redacted] replies to him on the 19th of February 2019 that it has deleted all "non-vital" information regarding the petitioner. [redacted]

implemented the hash verification mechanism on the 2nd of July 2018, date when the second account created by Mr. [redacted] was anonymised an the first account was completely deleted;

7. by accessing the website [redacted] it is allowed to install cookies belonging to third parties such as: _ga, _gat, _gid (Google Analytics cookies that allow the tracking of the browsing behaviour of the users on the website and helps to improve the use of this website), _fbp (cookie used by Facebook for the purpose of "Targeting/Advertising"), some of them having a validity period longer that that related to a session of use of the website;
8. although a banner containing a text (exclusively in English) regarding the use of cookies ("We use cookies to operate our website as expected and for performance and analytics purposes. By using our website, you agree to our use of cookies as described in our Cookie Policy") and a button for accepting them ("I accept") are available on the first page, it is noted that, after browsing various pages of the website, the cookies are installed on the user's terminal device, although it does not access beforehand actively the button to accept the conditions regarding the use of cookies. Such way of obtaining the consent does not correspond to the provisions of Article 6 paragraph (1) of Regulation (EU) 2016/679, related to the definition given to the consent in Article 4 point 11 of the same act: "'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her". As such, they are not cumulatively fulfilled conditions imposed by Article 4 paragraph (5) of Law no. 506/2004 which provided the following:

"(5) The storage of information or gaining access to the information stored in the terminal equipment of a subscriber or user is allowed only if the following conditions are cumulatively fulfilled:
a) the subscriber or user concerned has expressed his/her consent;
b) the subscriber or user concerned was provided, prior to the express consent, accordance with Article 12 of Law no. 677/2001, modified and amended, with clear and comprehensive information that:
(i) are to be presented in an easy-to-understand language and easily accessible to the subscriber or user;
(ii) are to include mentions about the purpose of the processing of information stored by the subscriber or user or of information to which he/she has access.
If the provider allows third parties to store or to have access to information stored in the subscriber's or user's terminal equipment, the information pursuant to points (i) and (ii) shall include the general purpose of the processing of this information by the third party and how the subscriber or user may use the settings of the Internet browsing application or other similar technologies to delete the stored information or to deny third party access to this information."

9. from the letter no. 22297 of the 7th of October 2019 it follows that the information collected using the cookies used by Google Analytics are automatically transmitted to Google, being "out of control" of [redacted];
10. regarding the _fbp cookie file, the representative of [redacted] stated that it is generated by Facebook Pixel and uses it in the marketing campaigns carried out on the social network, without the noting that an express consent of the users of the [redacted] website is requested in view of using this type of file.

No previous situation regarding the application of a administrative sanction/corrective measures against [redacted] was identified in the ANSPDCP's records.

The deed found:

On the date of concluding this minute, it was found that [redacted], with the identification data mentioned on the first page of the minutes, did not present evidence on obtaining the unequivocal consent of the users of the website belonging to [redacted] before allowing the storage of information or gaining access to the information stored on the user's terminal equipment, by using cookies having as purpose obtaining analytical and marketing information, thus infringing the

provisions of Article 6 paragraph (1) letter a) and Article 7 of Regulation (EU) 2016/679, by reference to the definition provided by Article 4 point 11 of this act.
This deed constitutes a contravention pursuant to Article 12 of Law no. 190/2018, by reference to the provisions listed in Article 83 paragraph (5) letter a) of Regulation (EU) 2016/679.

The sanction imposed:

Since in this case [redacted] carries out a cross-border processing, it become applicable the provisions of Article 60 of Regulation (EU) 2016/679, as well as of Article 16 paragraphs (3), (5), (6), (7) of Law no. 102/2005, republished, which provide for the application of sanctions/corrective measures by decision of the president of ANSPDCP, which is based on the minutes of finding and on the report of the investigative personnel.

II. RECITALS:

Having regard to the findings from the investigations carried out at [redacted] the information and comments sent by the other concerned supervisory authorities in IMI (cases Article 56 – no. 66211, Article 60 Informal consultation no. 71416, Article 60 Draft decision no. 118884),

The additional information sent by [redacted] with the letter no. 11954 of the 9th of June 2020, according to which:

- "the reason why the data have not been completely deleted, but are kept in pseudonymous form, is the prevention of fraud of our service and the unlimited exploitation of the Trial Period"; in this sense, the controller invoked Article 6 paragraph (1) letters a), b) and f) of the GDPR as a legal basis for the processing;
- the reasons why the controller continues to process pseudonomysed data are the follows:

"- The malicious intent on the part of the user. It has abused our system repeatedly, as we have shows in our previous replies. In short, Mr. [redacted], after requesting the deletion of the original account, created a new account to benefit once again from the Trial Period, thus violating the Terms and Conditions of our service;
- The risk of company bankruptcy. If we do not take ay action against this type of behaviour, our service could be defrauded indefinitely. This would reduce the company's revenues and the possibility of developments and maintenance and, in the long run, would lead to the closure of the service and its withdrawal from the market. We mention that this mode of operation, widely used, would close any online service based on subscription;
- We respect the fundamental rights of the user. We do not infringe any of his fundamental rights, as required by Article 6, paragraph (1) letter f), cited above; their observance allowing the further processing of personal data in accordance with the legitimate interests of our service. This data is not used for any other purpose such as marketing or profiling and is not transmitted to another processor or third party. They are only used to verify a potential fraud."

- the information of the data subjects is made as follows:

"To create a [redacted] account each user shall agree with the Terms and Conditions and the Privacy Policy of our company. This involves reading these provisions and is done by checking a box on the Sign Up, representing the user's consent to the processing of personal data. It is an Internet standard used by most online services."

Under Section "Terms and Conditions" ([redacted]) it is mentioned:
"You may not and you agree not to enable others to [...] try to extend the Trial Period [...]. We reserve the right to terminate any account which is responsible for such violations. Any [redacted] agency account associated with it will be prevented from further use in the Application."

Under Section "Privacy Policy" ([redacted]) it is mentioned:
"We also store your agency usernames and emails associated with the Application email to prevent them being used on a new Application account and exploit the free trial period indefinitely. In case of account deletion this data will be anonymized by hashing."

- the procedure for anonymising the data relating to the accounts is as follows:

" a. The deletion request is registered and a case is opened
b. The data protection officer (DPO) takes over the request Ofițerul
c. The entry in the database is identified
d. The username fields in both tables containing personal data of the user are pseudonymised by hash method
e. Personal data fields password, first_name, last_name, address, postcode, city, country, country_id, company_name, vat_number, customer_id, plan_id, subscription_id, subscription_status, beta are completely deleted and take the value NULL
f. The user is informed by the DPO that his account has been deleted and the case is closed"

- the destination of the inactive accounts was explained as follows:

"Inactive accounts remain stored in our database during the operation of the service, aspect which is mentioned in the Privacy Policy:
'We also store, for the duration our service is active, your agency usernames and emails associated with the Application email to prevent them being used on a new Application account and exploit the free trial period indefinitely.'
When an user requests the deletion of his account, we initiate the "anonymisation procedure" described above.

The "Privacy Policy" also mentions the following:

"An account is deemed inactive if no activity is registered in the past three years. The personal data associated with such an account will still be stored on our servers, for the duration of our service, to prevent exploiting the free trial period, as detailed above."

Recital (47) in the preamble of the GDPR, according to which the processing of data for preventing fraud constitutes a legitimate interest of the data controller,

The storage of data related to inactive accounts during the functioning of the service, for a period that does not correspond to the purposes of the processing, pursuant to Article 5 paragraph (1) letter e) of the GDPR,

The use of pseudonymisation method (hash MD5) which is considered to present some risks of re-identifying the data subjects (see in this respect the Opinion of WP29 no. 5/2014 on the anonymisation techniques, WP 216 of the 10th of April 2014, p. 21-22),

Given: the number of data subjects (55 active [redacted] clients); the receipt of a single complaint from a single data subject (from Germany); the reasons presented by the controller to legitimately justify the retention in encrypted form (MD5 hash) of the personal data associated with a deleted account in order to avoid the creation of a new free account (only valid for one month); information of the data subjects available on the website; the remedied made by the controller during the investigation; the use of cookies belonging to third parties (Google, Facebook) through the website [redacted] for analytical and marketing purposes, without first obtaining the consent of the users of the website,

The unfounded character of Mr. [redacted]'s complaint, under the aspect of requesting the erasure of his personal data,

Having regard to the provisions of Article 5 paragraph (1) letter e), Article 6 paragraph (1) and of Article 7 of GDRP, related to the definition from Article 4 point 11 of GDPR regarding the conditions under which the processing of personal data can take place based on the consent of the data subjects, as well as of Article 4 paragraph (5) of Law no. 506/2004 regarding the legal conditions in which it is allowed to store information or to gain access to the information stored on the terminal equipment of a subscriber or user, as well as of Article 32 of the GDPR,

Taking into account the case law of the Court of Justice of the European Union, in particular, the Judgement of 29th of July 2019 in Case C-40/17 ("Fashion ID") regarding the obligation of the administration of a website to obtain the consent of its visitors and to ensure the information of the data subjects with respect to the processing of personal data, in case of insertion of a social module

that allows the visitor browser to request content from the provider of this module, but also the one resulting from the Decision of the 1st of October 2019 in case C-673/17 ("Planet49"), regarding the obligation to comply with Article 5 paragraph (3) of Directive 2002/58/EC (transposed in Romania by Law no. 506/2004), in the sense of enabling the user to express his/her free consent, after being provided with clear and complete information, in relation to the storage of information or to the acquisition of access to information already stored in a user's terminal equipments by means of cookies, consent which has the same meaning as the consent referred to in Article 6 paragraph (1) letter a) and Article 4 point 11 of the GDPR, expressed through an active behaviour, a manifestation of the "free, specific, informed and unambiguous" will of the data subject, in the form of a statement or an "unequivocal action" (see, for example, paragraphs 46, 50, 54 and 61 of this judgement),

Pursuant to Articles 14, 15 and 16 of Law no. 102/2005, republished, of Article 12 of Law no. 190/2018 related to Article 83 paragraph (2) and to the provisions listed in Article 83 paragraph (5) letter a) of Regulation (EU) 2016/679, corroborated with the provisions of Article 58 paragraph (2) letters b), d) and f), as well as of Article 60 of Regulation (EU) 2016/679, related to the provisions of Articles 24, 25 and 26 of the Procedure for carrying out investigations, approved by the Decision of the president of ANSPDCP no. 161/2018,

Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal

ORDERS

the following measures against [redacted]:

1. Issuing a reprimand for the fact ascertained through the minutes no. 17062 of the 24th of August 2020, based on Article 58 paragraph (2) letter b) of Regulation (EU) 2016/679;
2. Imposing the corrective measure provided by Article 58 paragraph (2) letter f) of Regulation (EU) 2016/679 to temporary limit the use of cookies belonging to Google and Facebook, until the correct implementation of a method for obtaining the prior express and informed consent of the users of the website [redacted] for this purpose, pursuant to Article 6 paragraph (1) letter a) and Article 7 of Regulation (EU) 2016/679, by reference to the definition provided by Article 4 point 11 of this act and Article 4 paragraph (5) of Law no. 506/2004;
3. Imposing the corrective measure provided by Article 58 paragraph (2) letter d) of Regulation (EU) 2016/679 to implement a method of anonymisation to prevent the risk of re-identification of persons whose personal data are subject to this procedure, pursuant to Article 32 of Regulation (EU) 2016/679 – deadline: 20 working days from the date of communication of this decision;
4. Imposing the corrective measure provided by Article 58 paragraph (2) letter d) of Regulation (EU) 2016/679 to establish a limited duration (less than 3 years) for the storage of data related to inactive accounts and to apply, in their case, the anonymisation method used also in the case of active accounts, at the expiry of the period mentioned previously, in order to comply with the principle provided by Article 5 paragraph (1) letter e) of Regulation (EU) 2016/679 – deadline: 10 working days from the date of communication of this decision.

[redacted] shall communicate to ANSPDCP the measures adopted for the implementation of the corrective measures within 45 days from the communication of this decision.

This decision was subject to the procedure provided for in Chapter VII of Regulation (EU) 2016/679, being sent for approval to all concerned supervisory authorities.

This decision, together with the minute no. 17062 of the 24th of August 2020 shall be communicated to [redacted] that has the right to challenge them pursuant to Article 17 of Law no. 102/2005:

”Article 17
(1) The data controller or processor may file an appeal against the report of the finding/sanctioning and/or the decision to apply the corrective measures, as the case may be, with the administrative contentious section of the competent court, within 15 days from handing, respectively from communication. The decision resolving the appeal can be appealed only by appeal. The appeal is judged by the competent court of appeal. In all cases, the competent courts are those in Romania.
(2) The report of finding/sanctioning or the decision of the president of the National Supervisory Authority unchallenged within 15 days from the date of handing, respectively the communication, constitutes an enforceable title without any other formality. Introducing the appeal provided in paragraph (1) suspends only the payment of the fine, until a final court decision is issued.
(3)The deadline of payment of the fine is 15 days from the date of handing, respectively from the date of communication of the minutes of finding/sanctioning or of the decision of the president of the National Supervisory Authority.”

President,

[redacted]