Our ref.: **11.17.001.010.007** **4 October 2023**

Decision

Requesting Excessive Identification Information to Comply to a Subject Access Request by Technius Ltd

A complaint was lodged with the Netherlands DPA against Technius Ltd (the controller), whose main establishment is in Cyprus. Moreover, the complaint was subsequently transmitted to the Office of the Commissioner for Personal Data Protection (Cyprus SA) on 23/12/2021, in line with Article 56 of the General Data Protection Regulation (GDPR).

2. On the basis of the above, the Commissioner for Personal Data Protection (the Commissioner) is acting as the lead authority in this matter. In the course of the investigation, other EU countries were identified as being concerned by this case.

Description of the case

3. The complaint was filed against Technius Ltd which manages the website stripchat.com that sells live access to nude models. The complaint included the following information:

3.1. The complainant was informed through online media that the website StripChat had suffered a data breach. Following this, he searched his mailbox and discovered that on 22/10/2019, someone other than himself, registered/created an account at StripChat using his personal email account. He then contacted the controller through the support email address help@stripchat.com on 17/11/2021, requesting to receive a copy of his personal data held by the company, following the provisions of Article 15 GDPR. Additionally, he enquired whether his personal data was affected by the above data breach.

3.2. On 01/12/2021, the controller replied via email address legal@stripchat.com, informing him that in order to proceed with his request, he had to submit a government issued identification document, to verify the identity of the person requesting the data. In his reply, the complainant insisted that requesting a government ID would be excessive since he has made a request using his email address and thus no further identification would be required.

3.3. The complainant was further informed that the data which was processed by the controller and was related to his email address, was the IP address and username that was collected during the account registration. The controller also

mentioned that if the complainant wanted to receive a copy of these data, they need to identify him, or alternatively, they could remove the said data completely from their system.

3.4. The complainant replied and stated that someone else had created the account on StripChat using his email and also that he was not notified of the data breach He also refused to provide any copy of identification document. The controller in their response, informed the complainant that the account would be deleted as it was created fraudulently and also referred him to the notification of the data breach on the website's blog post.

3.5. The controller also informed him that due to the nature of the incident, they were not in a position to identify the exact data that was affected by the breach. The complainant responded that he could confirm that his personal data was affected by the breach through an alert he got by the SpyCloud service.

4. In summary, on the basis of the allegations of the complainant, the controller:

i. only made a public announcement through a blog post, instead of personally informing him through email, and through the blog announcement he could not determine whether his personal data was affected by the incident,
ii. has processed incorrect personal data and stored it for more than two years,
iii. requested him to submit an identification document in order to fulfill his access request.

Investigation by Cyprus SA

5.1. The Commissioner's Office contacted the Controller on 11/2/2022, and requested their views on the matters raised by the complainant and, among others:

i. The reason for not informing each data subject individually about the breach.
ii. The legal basis under which an identification document is required to respond to a data subject's access request, or any other right (e.g., right to erasure, to rectification, etc.).
iii. The reason for not satisfying the data subject's request by providing the information directly to the connected email.

5.2. In their reply, the controller stated the following:

i. The data breach was deemed is likely to result in a high risk to the rights and freedoms of the affected data subjects. Moreover, the controller chose to inform their registered users through the website blog post taking into consideration:
    - That there was no indication of how many and which users were affected by the breach and

- the very large number of registered emails which would take approximately 5 months to inform by individual emails.

ii. As regards the identification documents requested,
- the procedure for requesting identification documents is only for data subject access requests,
- the purpose is to protect user data from unauthorized disclosure,
- the identification documents are deleted after verifying the identity,
- the email address is not a sufficient security measure,
- the identity is authenticated by comparing the identification document with existing records or billing information,
- the procedure follows the GDPR requirement of using reasonable measures to verify the identity of the data subject (Recital 64 GDPR).

iii. The complainant's access request was considered as satisfied since the controller provided all the necessary information and explanations with regards to the account opened under his email address as well as all the information that could be provided about the incident.

5.3. The Commissioner's Office took into account the above facts and information, the comments from concerned supervisory authorities, and noted the below:

i. It was considered that a blog post was not sufficient for the communication of the data breach to the affected data subjects and thus the Commissioner immediately instructed the controller to proceed with sending an email to all registered users regardless of the effort and time needed. The controller complied with the instruction without delay.

ii. The account registered to the complainant's email address was active and thus the erasure of the data was not justified before the complainant contacted them.

iii. The registration process requires that the user confirms the registration by using a single-use password that is sent to his mailbox thus ensuring accountability.

iv. The complainant's email address was confirmed during the registration, which could only be done by a person with access to the specific email address. Considering that the complainant claims he did not perform the registration himself, it can be deduced that his email address was accessed by a non-authorized person.

v. When the complainant informed the controller that someone else used his email address to register, the controller informed him that in this case, the Username and IP address were personal data of the third party who opened the account by using his email address. Moreover, the complainant was informed about what type of data were related to the

account associated with his email address and was also informed that the account and the connected personal data would be deleted from the website database since the account was fraudulently opened.

Preliminary Decision

6. On 15 June 2023, the Commissioner issued a Preliminary Decision regarding the above investigation. In the said Preliminary Decision, the Commissioner concluded that:

a. The complainant's account was active and the controller was not aware that it was opened fraudulently. Therefore, the controller had no reason to erase the data before the incident.
b. There is **a breach of Article 5(1)(c) GDPR** (principle of data minimization) since the controller did not have a plausible reason to ask for a government ID from the complainant, specifically considering that:
    i. the controller requested the identification before they were notified by the complainant that the account was opened fraudulently,
    ii. the controller could not have used any government ID to identify the DS, since the controller does not already process any of the data types included in any government issued ID,
    iii. the complainant could have been identified through the linked email address without the need for additional identification documentation, and
c. there is **an infringement of Article 34(1) GDPR** since the controller did not communicate the personal data breach in an appropriate way.

7.1. The controller responded on 26 June 2023 to the Preliminary Decision and stated, inter alia, that:

a. The company has implemented further organizational and technical measures to guarantee full compliance with the GDPR.
b. With regards to the infringement identified under Article 5(1)(c) of the GDPR, the collection of identification documents procedure was only applicable to "access requests" and the intention was strictly to protect the data of the users from any unauthorized disclosure in accordance with Recital 64 of the GDPR. Nevertheless, this procedure has been abandoned and the email verification will be used as a sufficient measure to verify the ownership of the personal data in question.
c. With regards to the infringement identified under Article 34(1), at that time it was considered the public announcement through the website blog was the most suitable and efficient measure to inform the affected users. In addition, the process of contacting each user personally through an email would have taken at least 5 months to be completed in comparison with the mass and immediate notice through the blog. Despite this, the controller complied with the Commissioner's instructions and proceeded with personal email notification as it was not their intention to avoid informing the affected users.

7.2. In addition to the above, the controller included the following mitigating factors to be taken into account by the Commissioner:

a. The controller immediately informed the Commissioner about the incident and took all reasonable steps to mitigate the impact on its users. In addition, it was and as of today is still in constant communication with the Commissioner.
b. Even though the company has been operating since 2016, it is the first time that the Commissioner or any other DPA authority receives a complaint about the company procedures regarding GDPR.
c. The controller complied with all the requests of the Office of the Commissioner for Personal Data Protection without any delay and consulted the Commissioner during all steps to ensure compliance with GDPR.
d. Actively improved its security measures and internal processes as per the guidance and recommendations of the Commissioner. It informed its users through direct email communication in addition to the public announcement initially made and changed its procedure regarding the access requests of the data subjects.
e. It is clearly evidenced from its immediate compliance with the Commissioner's requests that there was no intention to infringe either article 5(1)(c) or article 34(1) of the GDPR.

Legal framework

8.1. **Pursuant to Article 5(1)(c) of the GDPR** "*Personal Data shall be:*
…
(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
…"

8.2. **Pursuant to article 34(1) of the GDPR** *"When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay."*

8.3. **Pursuant to Article 58(2) GDPR**, *Each supervisory authority shall have all of the following corrective powers:*
…(b)to issue reprimands to a controller or a processor where processing operations have infringed provisions of 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;
…(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;

8.4. **Recital 86 of the GDPR** states that *the need to mitigate an immediate risk of damage would call for prompt communication with data subjects*.

Views of the Commissioner

9. Following the above facts and the response to my Preliminary Decision I note the below:

9.1. I recognise that the controller's intention for requesting an identification document was to protect any unauthorized disclosure. Despite this, as it is stated in recital 64, *a controller should not retain personal data for the sole purpose of being able to react to potential requests.* Thus, collecting identification documents solely for satisfying data subject rights is excessive, regardless of when the data is collected.

9.2. Additionally, I hold the position that the controller should have informed the affected data subjects more directly taking into consideration the nature of the breach and the categories of personal data affected. This is also strengthened by the fact that the controller regularly processes data concerning the sex life of its registered users.

Decision

10. Having regard to all the above information, and based on the powers vested in me by **Articles 58 and 83 of Regulation (EU) 2016/679 and article 24(b) of National Law 125(I)/2018**, I conclude that there is an infringement by Technius Ltd of **Article 5(1)(c) and 34(1)** of the GDPR, for the reasons mentioned above.

11. Moreover, following an infringement of Article 5(1)(c) and 34(1) GDPR, as explained above, under the provisions of Article 83 of the GDPR, I take into account the following mitigating (1-3) and aggravating (4-6) factors:

1. That there is no previous violation by the controller of the GDPR.
2. The controller complied with all the requests of the Commissioner without any delay.
3. The measures taken after the incident to ensure that all staff is appropriately trained in handling GDPR matters.
4. The controller should have taken appropriate and prompt measures in effectively communicating the breach to its users.
5. The complainant should have been identified using other less excessive means.
6. The controller should have implemented more appropriate procedures and measures considering the processing of special categories of data.

14. In view of the above and on the basis of the powers conferred on me by the provisions of subparagraph (b) of paragraph (2) of Article 58 of the GDPR, I have decided to **issue a reprimand** to Technius Ltd for the infringement mentioned in paragraph 10 above. In the event of a recurrence of a similar infringement within 12 months from today, this Decision may be counted against the company.

Irene Loizidou Nicolaidou
Commissioner
For Personal Data Protection