Report

of the Hungarian National Authority for Data Protection and Freedom of Information
on
the use of Yandex.Metrica analytical service applied on the website of the National Consultation

– short summary –

I.   Facts established by the Authority

The National Authority for Data Protection and Freedom of Information (hereinafter: Authority) learnt form press articles that data protection requirements might be contravened by using Yandex.Metrica analytical service on the website of the National Consultation https://nemzetikonzultacio.kormany.hu/. The Authority started investigation procedure in this matter, according to Section 38 (3) point a) of Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information (hereinafter: Privacy Act).

During its procedure, the Authority contacted the Cabinet Office of the Prime Minister and also Yandex LLC. (hereinafter: Yandex) who is the provider of the analytical service. The Authority also collected contracts and statements. Furthermore the Authority conducted on-the-spot examination at Trendency Online Zrt. (hereinafter: Subcontractor) which develops the website.

On this basis, the Authority found the following facts:

On 14 February 2017 the Cabinet Office of the Prime Minister concluded a framework contract with the consortium of New Land Media Kft. and Lounge Design Kft. (hereinafter: Contractor). The development of the website of the National Consultation was granted under this framework contract.

Before starting the development of the website, the Cabinet Office of the Prime Minister and the Contractor held several personal consultations, of which three short written notes, so called "briefs" were made. In these briefs, the Cabinet Office of the Prime Minister and the Contractor included professional conception and other expectations regarding the development of the website. From the "briefs" it can be stated that the Cabinet Office of the Prime Minister asked for "usage statistics" on the traffic of the website.

Subsequently, on 20 March 2017, the Contractor sent a quotation to the Cabinet Office of the Prime Minister, which also included the document "*Planned functionality/design*". This Annex outlined the content of the website by the Contractor. In the document entitled "*Analytics*", the following description was

added: "*An analytical tool is being built in, to create usage statistic of the traffic of the website, to analyze user habits.*"

The website was prepared by the Subcontractor under a framework contract with the Contractor. The Subcontractor stated that during the previous government projects, developers of websites have been using Google Analytics. However, the Subcontractor has listed a number of considerations as to why it is advisable to use the Yandex.Metrica service provided by Yandex. For example, it uses measures by different approaches compared to Google Analytics, and provides more specific information on user behavior. Yandex.Metrica also measures more accurately than Google when it comes to the usage of mobile devices (mobile phones, tablets).

The Authority found that the Cabinet Office of the Prime Minister did not instruct either the Contractor or the Subcontractor to use a specific and concrete analytical tool or even the Yandex.Metrica analytical service. Neither the Contractor nor the Subcontractor has informed the Cabinet Office of the Prime Minister that Yandex.Metrica service will be used. The Cabinet Office also became aware of the installation of the Yandex.Metrica service at the time of the press release.

According to the Subcontractor's statement, Yandex metering code was set up 1 to 3 days before the National Consultation website was launched. The employee of the Subcontractor who was advised to set up the Yandex measuring code, has created a separate Yandex account for the National Consultation website. The employee has first turned on the function "Session Replay, scroll map, and form analytics" in the Yandex account.

This setting included the sending of all first interactions of the user, such as personal data (name, e-mail address, age) provided during the National Consultation. Prior to launching the site, however, the subcontractor's project manager informed the co-worker that this function would not be needed, so it was disabled in the account. However, the staff member did not remove the relevant reference from the html code of the site ("WebVisor" module). This should have been manually deleted from the code so that the user's computer won't send personal information for Yandex. However, the employee of the Subcontractor did not know about this, so he thought it was enough to turn off the function on Yandex's server (Yandex account only).

The Subcontractor's project manager had not verified the Yandex settings since they only performed a functional test before launching the website. The Subcontractor did not specifically perform the test of analytical settings.

The Authority also contacted Yandex regarding the data flow conditions. Yandex emphasized in its reply that it has a decentralized data center system, so it has a data center in Russia, Finland and the Netherlands. According to Yandex, the user's machine is sending the data packet to the "nearest server" according to the network topology. For Hungary, this means in most cases the Netherlands.

Yandex explained to the Authority that if the "*Session Replay, scroll map, form analytics*" function on the Yandex account is disabled, but the Yandex metric remains active in the "WebVisior" module, Yandex will not store the data. According to Yandex, two weeks of data storage will be held only if "Session Replay, scroll map, and form analytics" function is also turned on in the Yandex account.

According to the information provided by the Cabinet Office of the Prime Minister, the National Consultation website was launched on 8 April 2017 at 9.07 am, and as a result of the articles in the press, the Yandex's code was removed at 10:45am on April 9, 2017 from the website. During this period a total of 11572 questionnaires were completed. However, the number of people involved cannot be determined precisely, as there is was no identity authentication. The system simply verified that the questionnaire could not be filled out twice with the same email address. For the authentication of the person filling in, additional person identification data (mother's name, place of birth, and date of birth) would have been needed which was not possible to provide.

II.   The findings of the Authority

1. Data processing at issue during the investigation procedure

The Authority found that the personal data included in the first step (surname, first name, e-mail address and user-specified age) was also covered by the data transmission. This is referred to the "Yandex Analytical Service Test" conducted by the Subcontractor on April 19, 2017.

The Authority considered from a data protection legal point of view whether the limited duration of the Yandex.Metrica analytical service was in line with the Privacy Act, and if not, whether it is a data incident and which and what level of liability it incurs.

2. Defining the data controller

According to the documents known in the case and of the Privacy Act, the Authority found that the Cabinet Office of the Prime Minister is considered to be an independent data controller regarding data processing through the National Consultation website. The Cabinet Office has full decision-making powers in terms of data processing, for example, the Cabinet Office has decided on the processing of data (the possibility of completing the National Consultation through the website), the essential circumstances of data processing (for example, the Cabinet Office has decided on the duration of data processing and on each purpose of the data processing). The Cabinet Office of the Prime Minister also states in the Privacy Policy that the Cabinet Office is considered as data controller.

However, defining the data controller in terms of using the service provided by Yandex.Metrica is different.

The Subcontractor has decided to use Yandex.Metrica's analytical service at the following website: www.nemzetikonzultacio.kormany.hu.
The Subcontractor's staff member set the metric code and the same person failed to disable the "WebVisior" module within the metric code. The subcontractor did not inform the Cabinet Office of the Prime Minister about the use of Yandex.Metrica so that the Office could not make a decision on using the tool.

As a result, for the data processing associated with the use of the Yandex metering code, the Subcontractor has ruled on all data protection issues and omission of liability has occurred in the Subcontractor's scope of responsibility . The Authority also stated that this decision of the Subcontractor was taken independently of both the Cabinet Office or the Contractor. Accordingly, the Subcontractor shall be considered as an independent data controller in connection with the use of the Yandex.Metrica service.
Based on the above, the investigation has not affected the Cabinet Office of the Prime Minister as a data controller.

3. The legality of the data processing

3.1 Data controllers have to comply with a number of obligations of the Privacy Act. They have to ensure that data processing is legitimate, such as having to comply with the principles of data processing (Section 4 of Privacy Act) and the legitimate grounds of processing (Section 5-6 of Privacy Act). According to Section 4 of Privacy Act, data controllers must examine whether the processing of personal data is necessary to carry out their intended activities. If a solution or a method is available, with which their objective may be attained without the need for data processing, then they must apply that method.

In the course of the procedure, the Authority found that the Subcontractor partially maintained the data protection requirements arising from this principle, as he intended to set up an analytics on the National Consultation website, which does not involve personal data handling.

However, the Subcontractor did not act with due care, as the "WebVisior" module remained active in the Yandex metering code as a result of a professional fault of a colleague. This led to the data package sent by the user's computer to contain all the interactions that the user performed on the website (such as name, e-mail address and age the user has typed in). Due to the default the Subcontractor did not have a legitimate purpose and legal basis for data processing regarding this type of unplanned data processing.

In addition, the Authority also found that the Contractor was also liable in that it could have verified Yandex's analytical setup or it could have required a data-protection control for the Subcontractor regarding Yandex.
Additionally, the Contractor could have specified in the "briefs" or in his price offer of 20 March 2017, what analytical services could be used and what settings they can use on the website. Therefore the Subcontractor could have developed the website accordingly.

3.2 One of the features of the data processing under investigation is that Yandex provides its analytical service through servers in Russia. On the basis of the code, the Authority found that the metric code sends the data to the direction of a server located in the territory of the Russian Federation.

However during the investigation, Yandex claimed that in case of a Hungarian user, the server, which is located in the Netherlands, will receive the data. In addition, Yandex also claims that since the Yandex server (Yandex account) was turned off, the data was not received by its Dutch server.

In the course of the Authority's proceedings, neither objection nor reference to Yandex's statement was found and the functionality of the code did not show that, too. The Authority notes that such substantiation is not possible without the screening of foreign servers. In addition, the Authority emphasizes that Yandex's statement, that the feature was switched off for storing data, was also verified by an on-site inspection at the Subcontractor, as there were no data in the Yandex account.

3.3 Finally, in the context of the case, the Authority points out that the failure of the Subcontractor described in the report should be interpreted as data incident described in Section 3 point 26 of Privacy Act, as incorrect settings of the Yandex.Metrica service have led to unlawful data processing.

Privacy Act creates obligation to keep records of data incidents. According to Section 15 (1a) of Privacy Act, *data controllers – by means of an internal data protection officer should they have appointed one and with a view to control measures relating to data incidents and to inform data subjects – shall keep records containing the personal data affected, the personal scope affected by the data incident, the time, circumstances and effects of the data incident and measures taken to eliminate thereof as well as other information determined by law.*

During the investigation, the Authority found that the Subcontractor had no record of this data incident therefore it did not comply with Section 15 (1a) of Privacy Act.

III.   Legal effects

As a result of the investigation of Yandex.Metrica's analytical service with limited functionality and duration, the Authority requires the Contractor and the Subcontractor to take measures to prevent a similar data incident in the future.

At the same time as the disclosure of the report, the Authority invited the attention of all organizations involved to the following:

When they wish to use an analytical service:

-   in the future, in a contract or quote for the development of the website, it should clearly be indicated, which service provider's analytics will be

used. Also, the planned settings should be set out in the contract (especially the fact that the production of the analytics does not involve personal data processing).

- an effective privacy-control mechanism should be developed in conjunction with the analytical service used on the website, with which prior to the launch of the site, it can be guaranteed that the use of analytics does not involve personal data processing.
- in accordance with the Privacy Act, the recording of future data incidents should be achieved.

Budapest, 27.07.2017