Case no.: NAIH/2020/789/ Subject: closure proceedings
Official in charge: [redacted]

The regulatory inspection launched by the Hungarian National Authority for Data Protection and Freedom of Information (hereinafter referred to as NAIH) on 28th of November 2018 in relation to the obligations of [redacted] (hereinafter referre
2016/6791 ('GDPR') concerning the data breach notified to the NAIH on 16th of November 2018, was closed by the Authority with the attached notice.

Please note that, based on Section 20 (1) of General Public Administration Procedures (hereinafter referred to as Ákr. Act), the official language in administrative proceedings is Hungarian, therefore the official version of the notice is the Hungarian, attached to this letter. However, in order to facilitate and accelerate the procedure, we hereby provide you with the summary of the relevant provisions of the notice in English language, for your information.

In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

On 28th of November 2018 the NAIH launched a regulatory inspection in relation to the data breach notified by the Controller since the information given in the notification was not sufficient to assess whether the Controller had fully complied with the provisions of Articles 33-34 of the GDPR.

Based on the data breach notification and the Controller's answers to the questions asked by the NAIH, the following could be established.

The Controller notified the NAIH on 16th of November 2018 that on 2nd of November 2018 it received an e-mail message from an ethical hacker. The e-mail contained information which alluded to the hacking of the Controller's database. Since no other information was available for the Controller it wished to make certain that the hacker's allegations are correct and an unauthorized access to the system had indeed taken place.

Therefore, on 2nd of November 2018 the Controller launched an internal investigation, and commissioned an external expert as well with the execution of a vulnerability test. A blackbox vulnerability inspection was also initiated on 9th of November 2018. As a result, it was determined that the data breach occurred via an SQL Injection through the website [redacted] and the fact that an unauthorized access happened

[1] 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

The affected databases are related to different operative applications, and the personal data affected are those of employees (e.g. name, e-mail address, username, coded password), athletes applying for sponsorship (e.g. name, height, birth data, weight), Facebook contest winners (e-mail address, name address), persons enquiring via the website (contents of the letter, e-mail address, city, phone number, name) and individuals applying for salesclerk vacancies (name, e-mail address, phone number). The breach may affect 80 individuals, some of whom reside in Member States other than Hungary: Poland – 10 individuals, France – 8 individuals, Spain – 3 individuals, Germany – 2 individuals, Portugal – 1 individual, Denmark - 1 individual.

Judging by the log files the intruder called down only 1-2 data lines from each of the 17 affected data tables, as proof for the detected vulnerability and in hope of a future cooperation with the Controller. He / she neither blackmailed nor threatened the Controller, has not made the data public, and the Controller is not aware of any data transfer having taken place. Considering the circumstances of the case, especially the wording of the letter sent by the hacker to the Controller, the Controller decided that the breach is unlikely to result in a high risk to the rights and freedoms of natural persons, and did not communicate it to the affected individuals.

The controller has internal rules for the handling of data breaches. In this particular case, the IT Department, the data protection officer and the senior management all took part in solving the problem. The attacked system was protected by a firewall, direct access to the databases was possible only from certain IP addresses, and passwords had to be changed every 3 months.

After becoming aware of the data breach, the Controller inactivated the functions that allowed the attack. SQL Injection protection was introduced, and it encompasses all surfaces of the webpage now. No such problem was reported since. Furthermore, the Controller asked the attacker to delete the data gained from the system.

According to Article 32 of the GDPR the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. It is the Controller's task therefore - taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons – to implement the necessary measures in order to provide a secure processing environment.

Based on the circumstances of the case the NAIH concluded that the Controller has not implemented appropriate technical and organisational measures to ensure a level of security appropriate to the risk, therefore it has not fulfilled its obligation under Article 32 GDPR. This resulted in an unauthorized access the Controller's system and the personal data stored in it. NAIH **issues a reprimand to the Controller**, but, with regard to the facts that

- the hacker has neither blackmailed nor threatened the Controller, has not made the data public (he / she wanted to cooperate with the Controller in the future)
- after having become aware of the breach, the Controller reacted in time and with the right measures
- NAIH agrees with the steps the Controller took to promote the safety of its IT systems and prevent similar future attacks

deems that the reprimand is a sufficient sanction for the breach at hand and sees no reason to open an administrative proceeding as described in Section 60 of the Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information ('Privacy Act').

According to Section 38 (2) of the Privacy Act, the Authority shall be responsible to oversee and promote the enforcement of the rights to the protection of personal data and access to public information and information of public interest, and to ensure the free flow of personal data within the European Union. Section 38 (2a) of the Privacy Act, – which is also applicable in this procedure

– provides that the powers and responsibilities conferred upon the supervisory authority by the GDPR shall be exercised with respect to the legal entities falling within the scope of Hungarian law by the Authority in accordance with the General Data Protection Regulation, and with the provisions laid down in this Chapter and in Chapter VI.

According to Article 2 (1), the GDPR is applicable to the data breach notified to the NAIH. Based on Section 99 of Ákr. Act, the NAIH - within the scope of its competence - shall monitor compliance with the provisions of legislation, and the implementation of enforceable decisions.

Based on Section 7 and 98 of Ákr. Act, the provisions of the Act on administrative proceedings shall apply to regulatory inspections subject to the derogations set out in Chapter VI of the Act. According to Section 100 (1) of the Ákr. Act, regulatory inspections are opened ex officio and conducted by the authority in own motion proceedings.

According to Section 101 of Ákr. Act, where the regulatory inspection finds any infringement, the authority shall open proceedings, or if the infringement uncovered falls within the jurisdiction of another body, the authority shall initiate the proceedings of that body. Where the authority finds no infringement during the regulatory inspection conducted at the client's request, it shall make out an official instrument to that effect. In the own motion regulatory inspections, the authority shall issue an official instrument on its findings at the client's request.

Budapest, " " of January 2021

On behalf of [redacted], president of the NAIH:

[redacted]
Head of Department
Department of Authorization and Data Breach Notification