Case no.: NAIH/2018/4495/ /V Subject: **Final Decision**
Official in charge: [redacted]

Attachment: Notice no.: NAIH/2018/4495/ /V

The regulatory inspection launched by the Hungarian National Authority for Data Protection and Freedom of Information (hereinafter referred to as NAIH) on 18th of July 2018, in relation to the obligations of [redacted]) (hereinafter referred to as Controller or Group) based on Articles 33-34 of the Regulation (EU) 2016/6791 ('GDPR') concerning the data breach notified to the NAIH on 7th of July 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 18th of July 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 NAIH, the following could be established.

The Controller notified the NAIH on 7th of July 2018 that on 4th of July 2018 an attacker gained access to an employee's e-mail account and thus to the contact information - such as name, e-mail address and telephone number - of app. 800 colleagues, stored in the Controller's e-mail system.

The attacker was able log-in to th [redacted] ted e-mail address through the online available Outlook Web Application (OWA). In response, [redacted] Group Cyber Defence Centre (CDC) initiated its standard investigation and response proces [redacted] ntain the incident and understand the scope of the event.

The Group's network and system infrastructure was not compromised, the attack was limited to one e-mail account and its content. The forensic review conducted by the Controller's CDC professionals determined that the attacker viewed only a part of the contact list and e-mails. Based on the Controller's current understanding and the fact that the attacker tried to send out numerous e-mails, the attacker's primary goal was to use the compromised e-mail account to initiate a spam campaign. The spam campaign had a very limited effect due to the fact that the Controller's e-mail infrastructure only allows to send out a limited number of e-mails during a given time period. Following the detection of the attack, an internal e-mail was sent by the Controller, calling all colleague's attention to the phishing campaign.

[redacted] Group's Cyber Defence Centre disabled the compromised e-mail account, thereby removing the [redacted] er from the e-mail system as soon as the incident was identified. A group of information security and data protection professionals assessed the situation and determined the necessary actions. The

[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

account holder, whose account had been compromised, was given a new e-mail address and user name, and was also requested to change his passwords if he used it in his other accounts.

The rollout of multifactor authentication for Outlook Web Application is underway by the Controller. The implementation of this security measure will give an elevated level of security, ensuring that unauthorized access with a compromised password will be impossible without a second authentication factor which confirms the user's identity.

The data breach affected several colleagues residing in Member States other than Hungary. These Member States and the corresponding number of data subjects affected in that Member State are as follows: Austria – 1 person, Czech Republic – 4, Germany – 1, United Kingdom – 3, Croatia – 46, Italy – 14, Poland – 3, Romania – 11, Slovenia – 1, Slovakia – 68). The individuals affected were notified about the breach in their native language on 18th of July by the Controller.

Based on the circumstances of the case and the measures adopted by the Controller before and after the data breach occurred, the NAIH concluded that the Client has fulfilled its obligation under Articles 33-34 GPR concerning the data breach, and the procedure did not reveal any reasons to open administrative proceedings 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 September 2018

On behalf of [redacted] president of the NAIH:

[redacted]