Reykjavik, April 29, 2021

Reference: 2020010355/VIS

Decision

On April 29, 2021, the Icelandic Data Protection Authority (I. Persónuvernd) took the following decision in case no. 2020010355 (previously 2019020361):

I.

Procedure

1.

Notification of the data breach and initial communications

On February 15, 2019, InfoMentor, a company whose main activity is the development and operation of the online information system Mentor (the System), informed the Icelandic Data Protection Authority (the Authority) of a data breach via telephone. The System is intended for schools and other entities working with children, including nursery schools and elementary schools. One of the System's functions is to allow for information exchanges between schools and parents.

In the phone call, InfoMentor informed the Authority of its communications with an Icelandic information security company, Syndis, that took place in the afternoon of February 14, 2019. Syndis had contacted InfoMentor after receiving information that an unauthorised third party had gained access to the national identification numbers (I. kennitala) and avatars of hundreds of children through the System. The person responsible had contacted Syndis and informed the company of this vulnerability within the System. The Authority notes that the exact number of data subjects affected only became completely clear at a later stage and will be discussed in more detail below.

InfoMentor's account of the company's initial response after becoming aware of the data breach states that an action plan was activated immediately following the phone call from Syndis, which took place at 16:55 on Thursday, February 14, 2019. Following InfoMentor's analysis of the data breach, the company then informed the principals of every elementary school in Iceland of the data breach via email, between 16:45 and 16:55 on Friday, February 15, 2019. Later that day, between 17:41 and 19:33, InfoMentor then notified the schools whose students had been affected by the breach and specified the national identification numbers of the students in question. InfoMentor then sent them a more detailed description of the nature and scope of the data breach on Monday, February 18, 2019.

Between February 16 and March 4, 2019, the Authority received data breach notifications from 75 elementary schools and 9 nursery schools. The Authority notes that these notifications or other issues pertaining to these 84 schools are not the subject of this decision.

2.

Overview of the Authority's investigation and communications with InfoMentor

Following two phone calls on February 15 and 20, 2019, the Authority requested further clarifications and documentation on the data breach from InfoMentor with letters dated February 25, March 27, and May 10, 2019. The Authority received written responses from InfoMentor dated March 3, April 4, and June 4, 2019.

Having analysed the data breach based on the information at hand, the Authority requested supplementary data from InfoMentor via emails on January 13 and February 10, and a letter dated 23 March and reiterated on April 24, 2020. InfoMentor responded to these requests via emails on February 7 and 11, and with a letter dated June 1, 2020.

With a letter dated November 20, 2020, the Authority informed InfoMentor of its intent to consider imposing administrative fines on the company pursuant to Art. 46 of Act No. 90/2018, on Data Protection and the Processing of Personal Data, and Art. 83 of Regulation (EU) 2016/679 (the Regulation), due to InfoMentor's lack of appropriate technical and organizational measures to ensure adequate level of security of personal data. InfoMentor was afforded the right to be heard on the issue of possible administrative fines, as well as the case in its entirety, and responded with a letter dated December 11, 2020.

InfoMentor's views and explanations regarding each element of the case, as described in the aforementioned documents, will be discussed in the relevant chapters of the decision. Although not addressed specifically below, the decision takes all these documents and information into account.

3.

Procedure for cross-border processing

As indicated in InfoMentor's letter from March 3, 2019, the data breach affected one child in Sweden in addition to the ones affected in Iceland. Accordingly, the Authority notified supervisory authorities within the European Economic Area (EEA) of the data breach on August 12, 2019, through the Internal Market Information System (IMI). As indicated in the notification, the Authority considers itself to be the lead supervisory authority for this case and the Swedish supervisory authority, Integritetsskyddsmyndigheten (formerly Datainspektionen), to be a concerned supervisory authority, as defined by Recital 124 and Art. 4 (1) (22) of the Regulation, respectively. Within the timeframe given, Integritetsskyddsmyndigheten confirmed its position as a concerned supervisory authority.

On March 12, 2021 the Authority sent the draft decision to Integritetsskyddsmyndigheten through the IMI system, as Art. 60 (3) of the Regulation provides. Prior to this, the draft decision had been discussed at two meetings of the Board of the Authority, on January 28 and March 10, 2021. No objections were expressed within the four-week timeframe provided for in Art. 60 (4).

II.

Nature and scale of data breach

1.

Description of data breach

According to InfoMentor's letter dated March 3, 2019, each student's system number was visible in the URL for a particular page within the System, this six-digit system number being randomly assigned to each student without any connection to their national identification number. By creating a script for sending thousands of requests to the System, using random six-digit numbers, an unauthorised third party gained access to the national identification numbers and avatars of 423 nursery school and elementary school students in Iceland. According to the letter, the party in question had to be a registered user of the System and be signed into their account to be able send these requests. This was reiterated in InfoMentor's letter dated December 11, 2020. The letter was accompanied by, among other documents, a statement from InfoMentor's former chief technical officer which confirms that to exploit the vulnerability, it would have been sufficient to change the numbers in the URL address of the page in question.

In the letter, InfoMentor further described its analysis of the data breach. Among the company's findings was the fact that the third party in question was the parent of an elementary school student residing in Iceland's capital region and that they confirmed, in writing, that the purpose of their actions was to expose a vulnerability within the System. The parent also contacted another third party, a person with access to the System in Sweden, and requested that this person perform the same action. The person in question then accessed the national identification number and avatar of one child in Sweden. According to the Icelandic parent, no other data, except for those accessed by them and the person in Sweden, were viewed or downloaded. InfoMentor also states in the letter that in a written declaration, the Icelandic parent confirmed that they had deleted any pictures (avatars) that had been downloaded. As previously mentioned, the parent then alerted the Icelandic information security company Syndis, which in turn informed InfoMentor of the breach. The parent's notice to Syndis was accompanied by a technical analysis and a list of the national identification numbers of the children whose information had been accessed.

InfoMentor's letter from March 3, 2019 stated that the System's vulnerability had been fixed in the evening of Friday, February 15, or a little over a day after the company initially became aware of it. The System was then tested over the following weekend with an updated and improved version being released on Monday, February 18, 2019. InfoMentor also stated that the company accepted the Icelandic parent's account of their intentions and that the company's analysis of the data breach matched the information in the parent's statement and notice to Syndis.

In InfoMentor's letter dated December 11, 2020, the company further clarified that to access the avatars and national identification numbers, the persons in question needed to be signed into their System account. InfoMentor stressed that, according to both internal analysis and an external penetration test of the System, an unregistered user or other third party could not have exploited the abovementioned vulnerability to access this information. InfoMentor also explained that a solution for the vulnerability which caused the data breach had already been developed at the time of the data breach and that due to human error it had not yet been implemented. This then allowed for the vulnerability to be fixed as quickly as was the case after the data breach occurred.

InfoMentor's response to the data breach and the company's measures to ensure security of personal data will be discussed in more detail below.

2.

Scale of data breach – information accessed

As mentioned above and specified in InfoMentor's letter from March 3, 2019, the data breach affected 423 children in Iceland initially believed to belong to 96 different schools. Further analysis showed that 90 schools were affected and that only the children's avatars and national identification numbers were accessible but not their names, as originally had been assumed. Additionally, the data breach affected one child in Sweden as previously stated. InfoMentor reiterated this information in its letter from June 1, 2020.

On February 20, 2019, the Authority received an email from the parent of an elementary school student in Reykjavik stating that the child's photo metadata from the System included personal data of both the child and its parents, including their full names and national identification numbers. The Authority requested further information from the parent in question via emails on April 9 and 10, May 29 and June 3, 2019. The Authority also invited InfoMentor to comment on the issue of photo metadata within the System and thereby confirm the scale of the data breach. According to InfoMentor's letter dated June 4, 2019, the data breach did not in fact affect the child of the parent who raised the photo metadata issue. The company stated that further examination revealed that personal data was included in some photo metadata within the System. However, InfoMentor underscored that this did not apply to the avatars of any of the children directly affected by the data breach and reiterated this point in its letters to the Authority dated June 1 and December 11, 2020.

The Authority finds InfoMentor's documentation and explanations as regards the metadata to be sufficient to conclude that the data breach on February 14, 2019, only extended to national identification numbers and avatars of the affected data subjects.

3.

Lapses in InfoMentor's notices to nursery schools and elementary schools

In addition to the original data breach, which is the main subject of this decision, InfoMentor has informed the Authority of lapses in the notices of the data breach to certain nursery schools and elementary schools. InfoMentor's letter from March 3, 2019, affirms that two schools were only notified that the data breach had affected one of their students on March 1, 2019, over two weeks after the breach occurred. Moreover, the company sent students' national identification numbers to the wrong schools in a few cases, mainly in instances where the affected students had transferred to different schools and the information was sent to their previous schools. Furthermore, the national identification number of one student in Háaleitisskóli in Reykjavik had been sent to Háaleitisskóli in Reykjanesbær, a different municipality. InfoMentor states this last mistake can be attributed to the fact that the two schools were not sufficiently distinguished in the System even though they bear the same name. According to InfoMentor, the company notified the schools and persons who received information in error but did not send a notification of a data breach to the Authority.

InfoMentor's letter also states that the company mistakenly sent the data protection officer of the city of Reykjavik the national identification numbers of four students residing in a different municipality that were affected by the data breach. InfoMentor notified the data protection officers of both municipalities but did not notify the Authority of this data breach when it occurred.

In its letter dated December 11, 2020, InfoMentor states that due to human error the company did not send any formal data breach notifications regarding these instances. However, as explained in the letter, the schools and data protection officer who received national identification numbers in error were informed of that fact.

4.

Security measures implemented by InfoMentor and response to the data breach

In its letter to InfoMentor dated March 23, 2020, the Authority requested written information and data on how the company adhered to the requirements set out in Art. 32 of the Regulation regarding the security of processing. InfoMentor provided the requested information in its letter dated June 1, 2020, along with copies of risk assessments for the years 2018 and 2019, a memorandum dated March 29, 2019, confirming KPMG's work in relation to an audit on information security based on the main components of the System and a letter of completion regarding penetration tests carried out by the company Bulletproof on April 8-12 and 15-18, 2019. In the letter, InfoMentor stated that the company had already made the necessary changes to the System based on Bulletproof's report and recommendations. Moreover, structural and organisational changes had been made within the company in the year 2018 in order to increase security and efficiency. For example, management and staff responsible for technology and security had been replaced. In InfoMentor's letter dated December 11, 2020, the company also stated that internal procedures had been restructured in the previous two years and new and stricter ones regarding testing implemented in order to minimise the risk of human error. Lastly, InfoMentor has also stated that the company has had a designated data protection officer since the year 2017.

In its letter dated December 11, 2020, InfoMentor described actions the company had taken since the year 2017 to increase security within the System in more detail and provided further documentation, including a detailed list of around 370 technical tasks. The letter states that in the fall of 2017, the company formed a working group to methodically inspect the System as to the security of processing of personal data, the aim being to fulfil requirements of data protection by design and by default by the entering into force of the Regulation. InfoMentor states that the working group systematically went over all functions and filings within the System, which led to a number of improvements. InfoMentor's former chief technical officer confirms this in a written statement that accompanied the company's letter.

According to InfoMentor's letter from December 11, 2020, the company was aware of the vulnerability which led to the data breach and had ordered the creation of a solution for it. Such a solution was then programmed, but due to human error the task of introducing the solution had been marked as "completed" before the solution was fully implemented into the System. This is confirmed both in the former chief technical officer's statement and the list of technical tasks previously mentioned. InfoMentor specified that this allowed for the vulnerability to be fixed as quickly as was the case after the company became aware of the data breach.

From the information and data provided by InfoMentor, the Authority deducts that sufficient testing of solutions created to enhance the security of personal data within the System, such as the one for the vulnerability which led to the data breach on February 14, 2019, could have prevented

the data breach from occurring. The Authority also notes that the fact that InfoMentor only became aware of this mistake after the data breach points to inadequate follow-up and testing of the technical measures taken by the working group mentioned above.

III.

Decision of the Icelandic Data Protection Authority

1.

Scope of Act No. 90/2018 on Data Protection and the Processing of Personal Data and Regulation (EU) 2016/679

Pursuant to Art. 4 (1) and Art. 2 (1), respectively, Act No. 90/2018 on Data Protection and the Processing of Personal Data and Regulation (EU) 2016/679 apply to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

Personal data is defined in Art. 3 (1) (2) of Act No. 90/2018 and Art. 4 (1) of the Regulation as information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, genetic, mental, economic, cultural or social identity of that natural person.

Processing is defined in Art. 3 (1) (4) of Act No. 90/2018 and Art. 4 (2) of the Regulation as any operation or set of operation which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

The case at hand concerns a data breach in which an unauthorised individual gained access through the Mentor System to the national identification numbers and avatars of a total of 423 children in Iceland and in which another unauthorised individual gained access through the same system to the same data of one child in Sweden. Therefore, and as InfoMentor's main establishment is in Iceland, the case concerns processing of personal data which falls under the scope of Act No. 90/2018 and the Regulation and thus under the scope of the Authority's powers, as defined by Art. 39 of Act. No. 90/2018.

2.

Determination of controller and processor

Pursuant to Art. 3 (1) (6) of Act No. 90/2018 and Art. 4 (7) of the Regulation, a controller is the natural or legal person, public authority or other body which determines, alone or jointly with others, the purposes and means of the processing of personal data. A processor is an entity which processes personal data on behalf of the controller, as defined in Art. 3 (1) (7) of Act No. 90/2018 and Art. 4 (8) of the Regulation.

The Authority has previously addressed the relationship between InfoMentor and schools and other users of the System as regards the designation of a controller and processor, namely in the Authority's opinion dated September 22, 2015, in case no. 2015/1203. The Authority concluded that each of the System's users, e.g. schools, is the controller of the processing of personal data resulting from this use. Each user decides whether to use the System and if so, which personal data is entered therein and how. InfoMentor provides the System and thus acts as a processor of the personal data entered by each of the System's users. This determination is also consistent with the European Data Protection Board's Guidelines 07/2020 on the concepts of controller and processor in the GDPR.[1]

The Authority notes that this decision concerns solely the data breach within the System on February 14, 2019, and thus, InfoMentor's adherence to Act No. 90/2018 and the Regulation as regards the System and the company's subsequent response to the data breach.

3.

Security of personal data

3.1.

General requirements of Act No. 90/2018 and the Regulation

Pursuant to Art. 8 (1) (6) of Act No. 90/2018 and Art. 5 (1) (f) of the Regulation, personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures.

Chapter IV, Section 2, of the Regulation lays down rules and requirements concerning the security of personal data. According to Art. 32 (1), cf. Art. 27 (1) of Act No. 90/2018, the processor of personal data shall, taking into account the state of 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, implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; and (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

3.2.

Conclusion on the security of the relevant personal data in the Mentor system

It is undisputed that due to a programming vulnerability within the System, two unauthorised third parties gained access to the personal data of a total of 424 children in Iceland and Sweden on February 14, 2019. As stated in the description of the data breach above, human error led to the data breach since a solution for the vulnerability, that had already been created, had not been fully implemented. Insufficient follow-up and testing of security measures then led to this fact not being discovered until after the data breach had already occurred. Therefore, the Authority finds that in the case at hand, InfoMentor did not comply with the requirements of Art. 32 (1) (b) and (d) of the Regulation, cf. Art. 27(1) of Act No. 90/2018, cf. Art. 8 (1) (6) of Act No. 90/2018 and Art. 5 (1) (f) of the Regulation.

[1] Version 1.0, adopted on 2 September, 2020.

Additionally, InfoMentor did not ensure proper security of the personal data of the data subjects affected by the data breach when the company mistakenly sent national identification numbers to the wrong schools and data protection officer, and therefore did not comply with Art. 8 (1) (6) of Act No. 90/2018 and Art. 5 (1) (f) of the Regulation in these instances.

4.

Administrative fines – general conditions and considerations

Considering the Authority's conclusion and the number of data subjects affected by the data breach that occurred within the System on February 14, 2019, the Authority has evaluated whether administrative fines should be imposed on InfoMentor in accordance with Art. 46 of Act No. 90/2018 and Art. 83 of the Regulation.

As described above, InfoMentor was afforded the right to be heard on this issue. The company set forth its arguments in a letter dated December 11, 2020. In the letter, InfoMentor requested a further right to be heard on the intended amount, should the Authority decide to impose upon the company an administrative fine. The Authority notes that Art. 46 of Act No. 90/2018 clearly stipulates the range within which administrative fines can be decided, referencing both a minimum and maximum amount and when applicable, a maximum proportion of a company's revenue. Consequently, and considering the comprehensive right to be heard already afforded to InfoMentor during the investigation of this case, the Authority finds it clearly unnecessary to grant this request, cf. Art. 13 of the Administrative Procedures Act No. 37/1993.

Art. 47 (1) of Act No. 90/2018 and Art. 83 (2) lay down factors to which a supervisory authority shall give due regard when deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case. Each of these factors, as applicable to this case, will be discussed below.

4.1.

Nature, gravity and duration of infringement

According to Art. 47 (1) (1) of Act No. 90/2018 and Art. 83 (2) (a) of the Regulation, due regard shall be given to the nature, gravity and duration of the infringement taking into account the nature, scope or purpose of the processing concerned, as well as the number of data subjects affected and the level of damage suffered by them.

The data breach within the System on February 14, 2019, was an isolated incident involving two logged-in users of the System. The vulnerability, which allowed for unauthorised access to personal data, was fixed around 24 hours after InfoMentor became aware of the data breach. The breach affected 424 data subjects but there is no data showing any damage to them as a result of the breach. InfoMentor has stated that all personal data gathered in the data breach has been deleted. However, not only the data subjects known to have been directly affected by the data breach should be considered, but also those potentially involved. Based on the information at hand, the vulnerability could have affected any of the students whose information is stored in the System. The data breach directly affected students from 90 schools in Iceland and one in Sweden. Even though only a few students at each school were affected, this still led to unauthorised access to the personal information of 424 data subjects. Accordingly, the Authority notes that the number of data subjects that could potentially have been affected by the data breach is much larger than 424.

The fact that the vulnerability allowed for unauthorised access only for registered and logged-in users of the System affects the gravity of the data breach. In this respect, it must be noted that the System has several thousand registered users in Iceland. Nonetheless, a vulnerability allowing anyone, whether a registered user or not, to access the data in question would have increased its severity. It must, however, be noted that exploiting the vulnerability did not require any special technical knowledge, as explained in the description of the data breach. The Authority rejects InfoMentor's claims, put forth in several of the company's letters, that any such knowledge be needed in this respect. The Authority recognises that in order to create a script capable of sending thousand requests to the System, as was the case here, a higher degree of technical knowledge would be needed. The fact remains that using such a script was not needed to gain access to personal data within the System, as manually changing the system number in the URL address for the relevant page was sufficient.

4.2.

Intentional or negligent character of the infringement

The intentional or negligent character of the infringement shall be taken into account, as provided for in Art. 47 (1) (2) of Act No. 90/2018 and Art. 83 (2) (b) of the Regulation.

The Authority finds no evidence of an intentional character of the infringement. InfoMentor has conceded that a mistake led to the vulnerability in question. The Authority therefore views the data breach to be the result of negligence on behalf of InfoMentor as a processor of personal data.

4.3.

Actions taken by the processor to mitigate damage suffered by data subjects

Any action taken by the controller or processor to mitigate the damage suffered by data subjects shall be given due regard, as stipulated in According to Art. 47 (1) (3) of Act No. 90/2018 and Art. 83 (2) (c) of the Regulation.

As mentioned above, there is no evidence of any damage suffered by the data subjects affected by the data breach. The Authority notes that InfoMentor took immediate action when notified of the breach. However, these actions were lacking in accuracy and timeliness, cf. notifications that were sent to schools and a data protection officer in error and notifications to two schools that were only sent two weeks after the data breach occurred.

4.4.

Degree of responsibility of the processor – technical and organisational measures

According to Art. 47 (1) (4) of Act No. 90/2018 and Art. 83 (2) (d) of the Regulation, the degree of responsibility of the controller or processor, taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32 of the Regulation shall be taken into account.

InfoMentor, as processor, bears full responsibility for the System's vulnerability which led to the data breach. As previously described, a modification to the System necessary for eliminating this vulnerability had already been programmed but had not been implemented because of human error. The Authority notes that sufficient testing of such modifications could have prevented the data breach from occurring. In that respect, InfoMentor's follow-up of the technical measures taken to ensure the security within the System was not satisfactory.

The Authority also notes that a company, whose main business activity is the development and operation of an information system intended for schools and other entities working with children, should be held to a higher standard in this respect given the special protection afforded to the personal data of children in Act No. 90/2018 and the Regulation. Further increasing the importance of this is the fact that the processing of personal data within the System is at the core of InfoMentor's business activities.

4.5.

Degree of cooperation with the Icelandic Data Protection Authority

According to Art. 47 (1) (6) of Act No. 90/2018 and Art. 83 (2) (f) of the Regulation, due regard shall be given to the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement.

InfoMentor has cooperated fully with the Authority during the investigation of the data breach. The company has endeavoured to answer the Authority's questions clearly and has provided all requested documentation in a timely manner. On one occasion, the Authority had to reiterate its letter, but InfoMentor explained in its letter dated December 11, 2020, that this was due to the mishandling of mail after the company moved its headquarters in Reykjavik. The Authority accepts this explanation. However, the Authority finds InfoMentor's efforts to alert the respective controllers of the data breach to be inadequate, as regards the several lapses in these notices as previously mentioned.

As discussed above, there is no evidence of harm suffered by the data subjects affected.

4.6.

Categories of personal data affected

According to Art. 47 (1) (7) of Act No. 90/2018 and Art. 83 (2) (g) of the Regulation, the categories of personal data affected must be taken into consideration. In the case at hand, national identification numbers and profile pictures (avatars) were affected. Thus, no personal data falling under the definition of special categories of data, as defined in Art. 3 (1) (3) of the Act and Art. 9 (1) of the Regulation, were affected. Nonetheless, given the lack of adequate follow-up and testing of security measures within the System as well as the sheer volume of personal data of children being processed within it daily, happenstance rather than anything else seems to have determined which page and thus, which data, became accessible due to the vulnerability.

4.7.

Manner of notification of the infringement

InfoMentor, as processor, notified the Authority of the data breach. As provided for in Art. 47 (1) (8) of Act No. 90/2018 and Art. 83 (2) (h) of the Regulation, this will be a factor in the Authority's decision regarding administrative fines.

4.8.

Other aggravating or mitigating factors

According to Art. 47 (1) (11) of Act No. 90/2018 and Art. 83 (2) (k) of the Regulation, due regard may be given to any other aggravating or mitigating factors applicable to the circumstances of the

case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

InfoMentor did not stand to make any financial gains resulting from the data breach and as already discussed, no losses were incurred either by the company or the data subjects affected. The information and documentation provided by InfoMentor during this case indicate that the company's internal procedures were in certain ways lacking at the time of the data breach. However, InfoMentor has provided documentation showing steps the company has taken to prevent similar data breaches from occurring again. The company has also provided documentation showing considerable work from before the breach to enhance data security as can be seen by a detailed list of around 370 technical tasks that had been checked by then, albeit with the mistake that a solution that would have prevented the data breach in question had wrongly been marked as "completed".

4.9.

Factors not applicable to the case

Art. 47 (1) (5), (9) and (10) of Act No. 90/2018, cf. Art. 83 (2) (e), (i) and (j), on relevant previous infringements, measures ordered against the controller with regard to the same subject-matter and adherence to approved codes of conduct, are not applicable in this case. The Authority's previous opinions and decisions regarding the System, in particular its opinion in case no. 2015/1203 from September 22, 2015, mainly pertain to controllers' use of the System and their processing of personal data within it, rather than the security of the System itself, which is the subject of this decision.

5.

The Icelandic Data Protection Authority's conclusion regarding administrative fines

A conclusion regarding whether administrative fines shall be imposed upon InfoMentor in this case requires a balancing of all the factors discussed above. InfoMentor did not fully comply with the requirements of Act No. 90/2018 and the Regulation leading to the data breach which directly affected 424 data subjects, most of whom are children under the age of 18. InfoMentor's reactions to the data breach were in part inadequate as there were lapses in the company's notices to the controllers in question and in one instance, a data protection officer for a municipality. Moreover, given that InfoMentor's main activity is the development and operation of an information system intended for schools and other entities working with children, the company should be held to a higher standard in this respect given the special protection afforded to the personal data of children in Act No. 90/2018 and the Regulation, especially regarding adequate testing and follow-up of technical measures such as the ones that could have prevented the data breach.

However, there is no evidence of harm suffered by the data subjects. Only limited data became accessible, national identification numbers and photos (avatars), and there is no evidence this data was misused or manipulated in any way. The data breach was not the result of an outside attack, but actions of a logged-in user of the System. Accordingly, the personal data could not have been accessed or misused by a third party without an account within the System, which lessens the severity of the data breach. InfoMentor's responses and documents show the company has taken numerous steps to increase security within the System and improve internal procedures, both before and after the data breach occurred.

Having taken all the aforementioned into consideration, the Authority finds more aggravating factors of importance in this case than mitigating ones, in particular the number of data subjects

affected and the ones potentially affected, the fact the data subjects are children, whose personal data is afforded special protection in Act No. 90/2018 and the Regulation, and the degree of responsibility of InfoMentor as a processor due to the nature of the company. In light of these factors, as well as the fact that administrative fines shall be effective, proportionate and dissuasive, the Authority finds that an administrative fine in the amount of ISK 3.500.000 shall be imposed upon InfoMentor.

Conclusion:

The Authority finds that InfoMentor did not comply with the requirements of Art. 32 (1) (b) and (d) of the Regulation and Act No. 90/2018, cf. Art. 5 (1) (f) of the Regulation and Art. 8 (1) (6) of Act No. 90/2018, as regards the data breach on February 14, 2019.

The Authority finds that InfoMentor did not ensure proper security of the personal data of the data subjects affected by the data breach when the company mistakenly sent national identification numbers to the wrong schools and data protection officer, and therefore did not comply with Art. 5 (1) (f) of the Regulation and Art. 8 (1) (6) of Act No. 90/2018 in these instances.

The Authority orders InfoMentor, cf. Article 42 (3) of Act No. 90/2018, to implement specific procedures regarding responses to data breaches and the execution of security measures regarding processing of personal data, including regular testing of such measures. InfoMentor shall send the Authority a copy of these procedures within a month of the date of this decision.

An administrative fine of ISK 3.500.000 shall be imposed upon InfoMentor. The fine shall be paid to the State Treasury within a month of the date of this decision.