Case number: NAIH-85-3/2022 Re: Decision
Antecedent case number: NAIH-7350/2021

DECISION

On 22 September 2021, the **Nemzeti Adatvédelmi és Információszabadság Hatóság** (National Authority for Data Protection and Freedom of Information; hereinafter: the "Authority") initiated a data protection authority procedure ex officio against Budapest Bank Zrt. (registered office: 1038 Budapest, Váci út 193; hereinafter: the "Client" or in some of quoted texts the "Bank") in relation to the Client's data processing practices in connection with the audio recordings of telephone conversations made by the Client's telephone-based customer service between 25 May 2018 and the date of the launching of the present procedure. The Authority adopts the following decisions in the data protection authority procedure:

I. I. The Authority has found ex officio that the Client's data processing practices related to the analysis of the audio recordings subject to the investigation violated **Article 5(1)(a) and (b), Article 6(1), Article 6(4), Article 12(1), Article 13, Article 21(1) and (2), Article 24(1) and Article 25(1)** of Regulation (EU) 2016/679 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 (hereinafter: the General Data Protection Regulation, or GDPR).

II. Based on GDPR **Article 58(2)(d)**, the **Authority orders the Client ex officio to modify its data processing practices** in order to comply with the GDPR, i.e. not to analyse emotions in the voice analysis and to ensure that the data subject's rights in relation to the processing are adequately protected, in particular, but not limited to, the right to be informed and the right to object. With regard to Client's employees, the processing should be limited to what is necessary for the purposes for which it is intended and they should be provided with appropriate information, indicating the assessment criteria and the consequences. A separate interest assessment related to data processing related to employees with a different purpose must extend to the situation of exposure arising from this relationship of dependence and with regard to this, appropriate internal guarantees must be specified.

III. The Authority obliges the Client ex officio **to pay a data protection fine of HUF 250,000,000, that is, two hundred and fifty million forints.**

The Client shall provide the Authority with written proof of compliance with the obligation set out in Section II **within 60 days** of the date on which this Decision becomes final, together with the submission of supporting evidence. Data processing may be carried out only if an appropriate set of data is defined, a real impact assessment is done, a valid legal basis is provided with proof that the rights of the data subject are ensured to the maximum extent possible, otherwise the Client must provide the Authority with evidence of the cessation of the processing subject to the investigation within the above deadline.

The fine under Section III shall be paid **within 30 days** of the date on which this Decision becomes final to the Authority's Centralised Revenue Collection Special Account (10032000-01040425-

00000000 Centralised Collection Account IBAN: HU83 1003 2000 0104 0425 0000 0000). When transferring the amount, reference is to be made to the number “NAIH-85/2022 BÍRS.

If the Client fails to meet its obligation to pay the fine when due, it shall pay a penalty for delay. The rate of the penalty for delay is the lawful rate corresponding to the central bank base rate quoted on the first day of the calendar half year affected by the delay.

In the event of failure to pay the fine and the penalty and to meet the obligation according to Section II, the Authority orders the execution of the decision.

There is no legal remedy against this decision by the administrative route, but it can be challenged in an administrative litigation with a petition addressed to the Fővárosi Törvényszék (Budapest Municipal Court) within 30 days from its notification. The petition has to be submitted electronically to the Authority, which will be forwarded to the Court together with the documents of the case. A request for a hearing can be made in the petition. The duty of the administrative litigation is HUF 30,000 for those not benefiting from full personal exemption from duty; the litigation is subject to an objective right of prenotation of duties. Legal representation is mandatory in a procedure before the Budapest Municipal Court.

Pursuant to Section 61(2)(a) of Act CXII of 2011 on the Right of Informational Self-Determination and the Freedom of Information (hereinafter: Privacy Act), the Authority shall disclose this decision on its homepage.

JUSTIFICATION

I. The course of the procedure

I.1. Antecedent case

(1) Based on a complaint, the Authority examined data processing by the Client as a legal entity conducting the activities of a financial institution in antecedent investigative procedure NAIH-5161/2021 (hereinafter: Antecedent case), in particular, that the Client automatically analyses the sound recordings of calls to the Customer Service and whether the Client provides appropriate information to the data subjects in relation to this. Using the results of the analysis, the Client established which dissatisfied customer needs to be called back and in relation to this, it automatically analyses, inter-alia, the emotional state of the calling data subject, as well as the employee at the Customer Service, as well as other features of the conversation. In the Antecedent case, the complainant posed questions concerning the single sentence information referring to the analysis of sound recordings in the Client’s website, however, he did not receive answers satisfactory to him, hence he turned to the Authority.

(2) Called upon by the Authority, the Client made the following statements of merit in its response of 5 July 2021 filed under No. NAIH-5161-5/2021 in the Antecedent case, which the Authority qualified also in the present procedure in Section III of the Justification:

(i) The Client implemented the sound analysis application (hereinafter: Software) on 26.05.2017. The objective of the development was to improve the work of the close to 180 call centre staff, by improving the call selection procedure of the roughly 20 colleagues listening to the calls. Listening to previously recorded calls is affected by way of random selection even when the system is used, but the Software ranks the calls based on characteristics specified by the Software. These characteristics are not known even to the Client, they are managed by the Software as closed. The detailed results of call evaluation and the evaluation criteria are not accessible.

(ii) The objective of the Software is to render quality control more professional, to individually develop the Client's employees (both in terms of the profession and in communication), to improve the efficiency of processes and to boost customer experience. The system does not store any unique data or information on the customer suitable for identification. The data are analysed in aggregate. The areas of the use of the program do not include an improvement in sales results.

(iii) One of the main areas of use is the quality control of calls (listening-in): the analysis team selects the calls to be evaluated for those listening in. The selection criteria include data coming from the Software (e.g. dissatisfaction, disappointment, etc.). If needed, these parameters can be altered monthly with a view to making quality assurance as successful as possible and to enable them to uncover deficiencies and possible directions of development.

(iv) The second main area of use is the prevention of complaints and customer quitting: monthly a predetermined number of customers are called proactively with a view to preventing complaints, or eventual quitting. There are search conditions set in the system based on key terms, which assist in efficiently finding the customers concerned. This report can be run daily and the staff member listening in randomly can choose freely from among the potential calls.

(v) The third main area of use is efficiency improvement: group managers daily examine why there was a higher-than-average idling ratio (silence/music) and in which calls for their team. In exceptional cases, this is used for the individual development of staff members and the improvement of the efficiency of the processes.

(vi) The mandatory element of the notion of personal data, the possibility of associating the data with a specific natural person, is missing. The Software analyses the conversation, therefore no characteristic of the conversation can be established without listening to it again (which is a new data processing process).

(vii) The summary data enable only conclusions that can be drawn from the regulated business process, the conversations conducted based on script. The length of pauses and idling is not an indicator of individual talents even in the case of a given staff member, instead it indicates that special support is needed for the work. For instance, when the waiting time due to difficulty in accessing the IT system causes longer silence.

(viii) The Software is similar, for instance, to the operation of the traffic counter devices and traffic lights, which also determine the order of negotiating a crossing by natural persons participating in traffic, (who can otherwise be identified in other ways), yet their operation is not regarded as the processing of personal data in practice.

(ix) The purpose of data processing is the reduction of complaints and erroneous banking activities not objected to in a complaint ensuring efficient and courteous service to customers by supporting the efficiency of the control procedures as detailed above. The legal basis of processing is a legitimate interest of the Client detailed in the presentation of data processing purposes in terms of efficient and lawful case administration by phone. The period of data processing is 45 days with regard to sound recording that can be listened to within the Software and one year with regard to the statistics and ranked call lists generated through the operation of the Software.

(x) Software does not carry out any profiling that could be associated with an identifiable natural person, it ranks the calls as described above and generates call traffic summaries and statistics in a breakdown by the employees handling calls. It carries out automated processing operations with respect to the calls by ranking them. The result of the automated operation may be to increase or minimise the chance of being included in the random playlist for listening again through human selection.

(xi) […] operation of the sound recorder:

A […] records all sound materials by default. Every evening the server of the sound recorder automatically annihilates calls below 5 seconds. By default, every call is erased after 180 days, except for the calls, which have a business label, which are marked for “Long-term storage” in the setup tag of business label belonging to a given campaign in the / [...] interface.

A […] has a server dedicated for sound analysis, owing to which call recordings of within a day appear doubly. An automated program removes the sound materials of […] from the hit list. Irrespective of this, the calls can be listened to until the 45th day from their recording within the Software’s internal system. After this, the calls cannot be listened to within the Software.

(xii) Using the sound analysis function within the Software, it is possible to listen to and analyse the calls of the sound recording systems […] ([…]) […] and […] - […]. It is also possible to monitor and categorise the […] and […] calls made and received based on various quality criteria, the results of which enable the formulation of customer-specific actions and feedback with a view to improving customer service quality, recovery and the efficiency of sales. The individual members of functional management can receive data, which had not hitherto been measured with regard to quality for their entire area per area ([…]), per group and per administrator.

(xiii) The […], with the help of speech signal processing based on artificial intelligence:
• recognises on hold status / silence / simultaneous speech in sound files,
• recognises and finds keywords in the sound files,
• detects emotional / mood elements in sound files.

(xiv) The measurement of on hold / silence enables the head of the area to identify factors reducing efficiency and to take action both individually or at a level affecting the entire area (e.g. individual development, training affecting the area, process development, etc.).

(xv) Keyword recognition (based on a dictionary developed by us) enables the filtering out of complaining customers and the prevention of churn, as well as the presentation of prohibited / filler words.

(xvi) The detection of emotional / mood elements in the calls shows genuine customer experience or customer irritation.

(xvii) In its own storage, the Software stores sound files in an encrypted form for 45 days after which they are annihilated. Sound material analysis carried out earlier can be searched even after this, however, the call itself cannot be deducted from these .

(xviii) Automated decision-making in individual cases including decisions on profiling linked to a person is not carried out in the course of processing using the Software. Because of this, the conditions of GDPR Article 22(2) are not applicable.

(xix) The Client provides information to data subjects through Chapter 3 of its Rules of Business and the detailed Privacy Statement of its Phone-based Customer Service and complaint management, which were enclosed with the Client’s answer.

(xx) Ever since its implementation, the Software has been operating free of complaint.

(3) The Client provided the following evidence of merit in the Antecedent Case in the annexes of its response to the Authority's request filed under No. NAIH-5161-5/2021 received on 5 July 2021, which the Authority qualified also in the present procedure in Section III of the Justification:

(i) Internal memo concerning customer complaint […] (quotations verbatim)

"Prior to the phone call our Client received no information about analysing the conversation with the help of artificial intelligence and using a sound analysis software and, he would be curious about its purpose and the data processing purposes that this complies with.

He did not get an answer from the staff on Customer Service. I request the Privacy Statement and Rules of Data Protection related to this artificial intelligence software. Where can it be found? To what extent does it comply with GDPR?"

"I am sorry that our staff member was not aware of the relevant Privacy Statement: [link to intranet address]

Attach this to the answer. It should be underlined that the phone-based customer service carries out profiling for the purposes of quality assurance and complaint prevention based on legitimate interest and selects the calls by way of automated decision-making, in which a bank employee of higher qualification deals with the problem or complaint arising in the course of the phone call by way of returning the call.

The document referred to is accessible also at https://www.budapestbank.hu/hirdetmenyek/adatkezelesi-tajekoztatasok. It may be worthwhile noting that if our administrator would read out the general Privacy Statement (Chapter 3 of the Rules of Business) and the detailed data processing information referred to at the beginning of the call, this would extend the period of submitting a complaint or customer request by at least 10-15 minutes. This would be unacceptable to our customers. That is why the Bank decided to provide written information."

(ii) Internal memo concerning customer complaint […] (quotations verbatim, answer to another letter by the same data subject)

"[…] The software analyses the sound recording […] - according to criteria constituting the business secret of the developer. Of this, the developer presented the speed, volume, pitch and length of pauses in speech as examples. No profile is made as a result of the analysis, instead the system ranks the recordings daily. The ranking is based on whether the caller was dissatisfied with the service, although no formal complaint was made, as concluded from the aspects examined.. Calls at the beginning of the ranking are returned by a staff member having higher qualifications and authorisation attempting to remedy the reason for dissatisfaction. It follows from the closed operation of the system that the Bank does not have access to and does not process data other than the ranking of the calls. Thus, it does not transfer and store data, nor is it able to provide additional information on them. In the absence of a breach of security, the operation of the system cannot be regarded as a personal data breach. Exploration and prevention of latent complaints is in the common interest of both the callers and the Bank. This is the basis of the system's operation. In its current form, the preliminary information on data processing is adjusted to the expectations of GDPR Article 12(1), which requires concise and transparent information. The adequacy of this is indicated by the fact that our clients and non-client data subjects have not objected to this information over the past more than three years."

(iii) Identifier: H-407/2018 (Content of the detailed Privacy Statement Phone-based Customer Service and complaint management)

a) Phone-based customer service outgoing and incoming calls (in the form of a table)

processed data: name, address of notification, permanent address, mailing address, phone number (mobile, landline, workplace), e-mail address, mother's name, place and date of

birth, number of identification document (ID card number, passport number, driver's licence number), eventually income data, card co-holder, debtor, co-applicant, guarantor, lienee, personal data of proxy (name, date of birth, mother's name, number of identification document, etc.), account number, bankcard number, credit censorship / reference number, etc., insurance contracts, credits, savings, etc., data of transactions related to payment account, bankcards, credit card

Objective: to handle phone calls initiated by the customer (data subject)

Time frame: "See Rules of Business Section 3.1.8"

Legal basis: contracting in the case of incoming calls and "conscent" (*typo in the Hungarian original)* in the case of outgoing calls

Data processors: n/a

b) Phone-based customer service outgoing and incoming calls (in the form of a table)

processed data: name, notification address, phone number, client identifiers (account number, card number, etc), incoming channel, date of notification, complaint reference number, type of notification, is it a recurrent complaint, complaint category, in a given case the disputed amount, the severity of notification, antecedent complaint identifiers, detailed description of complaint, letter of complaint, other annexes, detailed resolution of complaint, in the given case credited amount, answer to complaint

Objective: management of complaint lodged by a client

Time frame: "See Rules of Business Section 3.1.8"

Legal basis: Contracting

Data processors: Partners (insurer, credit broker, etc.) needed for investigation

c) Other information at the end of the statement

See: data processing of the specific product concerned in the call or complaint on the data sheet of the given product.

The phone-based customer service carries out profiling for the purposes of quality assurance and complaint prevention based on legitimate interest and selects the calls to be returned by a bank employee of higher qualification to resolve the problems and complaint arising in the course of the phone calls by way of automated decision-making.

The Client is able to provide information on the recording, if any of the following data needed for identifying sound recordings is available:

• the data subject's phone number recorded by the bank providing call identifier service; in the absence of this;

• the phone number provided by the data subject providing call identification service;

• timeframe provided by the data subject specifying the beginning of the call with an accuracy of at least 60 minutes.

(iv) Identifier: H-526/2020 (Rules of Business, in force from: 10.01.2021, p. 41, quote)

"Section 3.1.8: Unless otherwise provided for by law, the general period of data retention is 10 years from the termination of the client relationship. This period of data retention is in line with the statutory limitation on general claims under civil law in view also of the break in statutory limitation. If the purpose of processing is the valuation of an eventual complaint, in the absence of a different provision by law, the period of processing is 1 year. These include, in particular, the data of claims for withdrawn or rejected services. The Bank may also take up contact with

data subjects having such transactions for marketing purposes until their consent is withdrawn. The period of storing video recordings for the purposes of asset protection is sixty days. The lawful period of retention of sound recordings for the purposes of complaint management is 5 years. Sound recordings containing the commissioning of a transaction is governed by the general period of data retention. The Bank blocks the data upon the expiry of the period of data retention, provided that the lawful conditions of blockage and the technical conditions enable this. The Bank may shorten the period of data processing, and excludes its liability related to this."

(v) Identifier: "interest assessment test, voicemining.xlsx" (in actual fact, a data sheet for data protection impact analysis)

Brief description of data processing: *"En masse sound analysis by software, search and analysis of predetermined content and key words and their transcription. Detection of emotions found in the sound file of the call (negative, positive)."*

Brief summary of the examination of necessity and proportionality: *"The processing of the data is needed for ranking calls according to the relevance of recalling. The ranking has no direct impact on the participants of the call. A re-listening carried out based on the ranking and the recall of the client (calling party) lodged as a result of this constitute a new, independent processing of data."*

The data protection officer's opinion and the summary of the decision on data processing: *"The purpose of processing is lawful, based on the rights of the data subjects and the business interests of the Bank, there is no direct or indirect legal prohibition. The processing is of high risk for several reasons, particularly in view of the novel nature of the technology applied as sound recordings are analysed automatically with the help of artificial intelligence and the statements are also made in an automated manner. The entirety of the data is suitable for profiling and scoring for both groups of data subjects and although no automated decision-making is carried out in the process, the processing may have a legal impact on the data subjects. The controller mitigates the high risk through the measures indicated in the impact analysis, for instance at the end of the automated processing, human decision-making is carried out. The exercise of data subject's rights is ensured according to standard practice. Exercise of their rights does not constitute a detrimental consequence for the data subjects. There is no processor in the process."*

(vi) Identifier: "adatvédelmi nyilvántartás kivonat.xlsx" (only the relevant parts highlighted)

Description: storage of audio files

Objective: The voice of the client is stored through the recorded calls. This can be listened to in the course of subsequent complaints or disputed cases.

Legal basis: Right, legitimate interest, interest assessment

Processing: no

Time frame: 10 years after the termination of the contract

(4) The Client made the following statements on the Antecedent Case in its response to the Authority filed under No. NAIH-5161-10/2021 received on 16 August 2021, which the Authority qualified also in this procedure in Section III of the Justification:

(i) *"Based on this, it can be established that the primary purpose of using the application is to facilitate the shortening of call time. The Bank's phone-based customer service capacity is limited. Because of this, the shortening of the call time can ensure to reduce waiting times giving rise to substantial client irritation or to terminate it together. The Bank achieves this purpose through*

analysing the pauses in conversation and listening to music during waiting time. In these cases, my colleagues process calls using statistical methods and listen to them only when necessary. Their purpose is to find the errors in the scripts directing conversations, which result in waiting, playing music or talking over the top of the other (the administrator and his talking partner cutting off each another). In such cases, the automatically ranked conversations selected for re-listening are not listened to in their entirety, but only partially based on the examined criteria. In this way, the employee listening in does not hear the client identification part. The application also supports the analysis of the same criteria by employee. This helps the employee within the system of performance-based remuneration to improve the success rate of his individual calls and reduce the time requirements of his calls."

(ii) *"The employee listening in can override the result of the screening at any time. The Software only provides a "menu" for the listener, from where he can choose, but in every case the decision is within the powers of the colleague performing the process."*

(iii) The Client annulled the employee consent attachment that was no longer used in operative work, and enclosed the rules in force ([…] - Bank group level instruction concerning the recording, listening in and processing of phone calls) and in addition to rationalising annexes, the Client also updated the organisational changes.

(iv) The Software is not a call recording system. This task is carried out by […] and […] systems. Calls are uploaded to the Software system from these. The data content of the Software includes the call identifier generated in the call recording system, the calling/called phone number, the direction of the call, its date and length, the name of the administrator, his organisational unit, the time and date of analysis, its quantified (%) results, the alphanumeric transcription of the recognised linguistic elements.

(v) The process of calls for client retention or complaint prevention

- The employee listening in starts a screening for the time period selected by him based on the rules and keywords set in the system.
- The Software lists the hits, i.e. the calls that match the filtering criteria.
- The employee randomly chooses from the recommended calls and listens to them (typically listening in to the part of the call indicated by the Software). If this substantiates the circumstance indicated by the Software, it is worthwhile to listening to the entire call.
- Having listened to the call, the employee decides whether client retention or complaint prevention is possible in the given case.
- If so, he calls the client having sought his data in the bank's systems.

(vi) Detected emotions can be displayed also at call level. They can then be combined at group and area level, and they can be ranked based on the strength of the emotion.

(vii) At the beginning of the calls, they do not provide information on using the Software, or on performing data processing for the purpose of voice analysis. If it is an incoming call ([…]), then the […] tells about sound recording. In case of an outgoing call ([…] and […]) the employee provides information on recording. If the client complains about the use of the software, the employees inform him of the possibility of recording the notification. If necessary, they take on the complaint to be investigated by the complaint management area, if necessary, also involving the data protection officer. We wish to note that the practical possibilities of providing verbal information at the beginning of phone calls are strongly limited. Information in a few words is necessarily misleading and force the data subject into an unfoundedly detrimental communication situation. Detailed, thorough information does not render compliance with the requirements of live voice contact according to the expectations of legal regulations and the supervisory authority. A

substantial part of the phone calls is about client's interests. Detailed information provided prior to answering a client's question about the opening hours of a branch or the current balance in his account would, by necessity, infringe the requirements of GDPR Article 12(1) concerning conciseness, because the time it would take, would by a multiple exceed the time taken on administering the case, the actual data processing.

(viii) The possibility of objection other than discontinuing the call is excluded by the technical conditions If the exclusion of a completed call from the analysis could be influenced by human intervention, this would significantly distort the efficiency of the analysis, since it is precisely in the case of calls containing anomalies that protests and administrative intervention are to be expected.

(ix) The Client provides information on the website https://www.budapestbank.hu/panaszkezeles.

(x) When the primary purpose of data processing ceases to exist, the Client deletes the data from its production systems, but Sections 3(3)(e) and (4) of Government Decree 42/2015. (III. 12.) referred to obligates the Client to create and manage archives, savings of data and back-up copies. The order of accessing them corresponds to the GDPR notion of blockage, hence the Client provided information on them in this way. The order of managing archive media can be found in the file management rules.

(xi) A Beyond the questions it is worthwhile underlining the experiences of personal checking that the signals of voice analysis concerning emotions are based on the features of the voice and the terms used, because of this they provide false results without human control. Also, there are people having voices (including some of our employees) whose voice always reflects dissatisfaction. In view of this, we consider the ratio of pose/speech into position and the speech/music ratio are relatively objective characteristics of a conversation, the emotional tone that is the experienced dissatisfaction and disappointment are less reliable characteristics. My colleagues pay particular attention to this when using the system.

(xii) The caller is only identified, if it is necessary to compensate him because of the Bank's fault, or the Client attempts to settle his latent complaint.

(5) The Client provided the following evidence of merit in the Antecedent Case in the annexes of its response to the Authority's request filed under No. NAIH-5161-10/2021 received on 16 August 2021, which the Authority qualified also in the present procedure in Section III of the Justification:

(i) Identifier: […] (Bank group level instruction concerning the recording, listening-in and management of phone calls)

"5. Detailed procedural order […]

Listening-in to recorded calls for the purposes of voice analysis:

With the help of the voice analysis Software within the software system, it is possible to listen-in to the calls of the voice recording systems […] and […] and their analysis at […] ([…]), […] and complaint management. Furthermore, it is also possible to monitor and categorise collection and […] initiated and received calls based on various quality criteria, and with the help of the results, we are able to formulate customer-specific actions and feedback with a view to improving customer service quality, recovery and the efficiency of sales*. The individual members of functional management can get quality related data, which had not been measured before for their entire area per area ([…]), per group and per employee.*

[…] recognises with the help of artificial intelligence-based speech signal processing:

- *waiting / silence / interposition in the sound files,*
- *recognition and finding key terms in the sound files,*
- *detects emotional / mood elements in the sound files.*

The measurement of waiting / silence enables the head of the area to identify the factors reducing efficiency and to initiate actions whether at individual or area level (e.g. individual development, training affecting the area, process development, etc.).

Keyword recognition (based on a dictionary developed by us) enables the screening of complaining clients, as well as the prevention of churn, and the finding of forbidden / filler words.

The detection of emotional / mood elements in the calls demonstrates genuine client experience or client irritation.

The Software stores sound files in an encrypted form in its own storage place for 45 days whereafter it erases them. It is possible to search for voice file analysis carried out earlier also after this, however, the call cannot be deducted from these."

(ii) Identifier: "érdekmérlegelési teszt voicemining_doc.docx"

"2.1. The specific, expressed and legitimate purpose of processing in line with Article 5(1)(b) of the General Data Protection Regulation: in the course of phone-based administration to reduce call time and to more efficiently filter out latent client complaints by way of analysing the characteristics of calls and improving the efficiency of listening into calls.

2.2. Presentation of legitimate interest: in accordance with Article 6(1)(f) of the General Data Protection Regulation, the processing of the data is necessary for the efficient enforcement of the legitimate interests of the Bank defined as facilitating the exercise of data subjects' rights by way of phone-based administration of their affairs.

3.1. The necessity of processing in line with the purpose according to Section 2.1: the checking of the calls by the controller and the optimisation of the data processing processes are necessary with a view to the fair procedure according to GDPR Article 5(1)(a) and accuracy according to point (d) of the same paragraph ensuring that erroneous administration of cases not explored in other ways are remedied.

3.2. Proportionateness of processing in line with the purpose according to Section 2.1 in view of the interests, rights and freedoms of data subjects: the Bank carries out the processing operations carried out with the help of this Software in accordance with GDPR Article 11 without identifying the specific data subject. The data subject is identified even in the case of a call listened in through random selection from the list generated by the software only if it becomes necessary to call him back.

The data subject cannot have any detrimental legal consequences in relation to the processing. A possible legal consequence is beneficial (remedying a complaint, ensuring crediting).

The Bank ensures proportionateness through the fact that there is only a low statistical chance for personalising the data generated in the system. A data subject need not necessarily expect to have a legal impact arising from the use of the system, there is little chance of that also in view of the purpose of processing.

3.3. Alternative solutions to substitute for processing: the controller does not have an alternative device procedure or solution available using which the purpose according to Section 2.1 could be achieved.

3.4. (Estimated) disadvantages and damage for the controller in the event of the omission of processing: reduction in the efficiency of calls, reduction in the efficiency of detecting latent complaints. The resulting increase in call drop-outs limits the ability of those affected to exercise

their rights to manage their affairs, including the protection of their personal data.. The reduction in the efficiency of detecting latent complaints reduces the accuracy of processing, which may give rise to financial or legal disadvantages for data subjects.

[…] 4.2. Favourable and unfavourable impacts of processing with regard to the data subject: the processing of the data has no independently unfavourable impact on the data subject.

4.3. Beyond the information mandatorily provided on processing, the data subject may request information on his data processed by the Bank, the purpose, legal basis and period of processing at any time (right to be informed, GDPR Article 12).

[…] 4.9. The data subject shall have the right to object on grounds relating to his particular situation at any time to processing of his personal data, including profiling based on the provisions of GDPR. In this case, the controller may not continue the processing of the personal data, except if the controller demonstrates that processing is justified by legitimate reasons of compelling force, which override the interests, rights and freedoms of the Data Subject, or which relate to the establishment, exercise or defence of legal claims.

[…] 6.1. Legitimate interests: It is an undisputable legitimate interest of the Bank to develop its phone-based customer service and detect latent complaints through the operation of its Software system.

6.2. The necessity of processing: the processing of personal data is indispensable for the achievement of the purpose of processing.

6.3. Assessment of proportionality: the data subject's right to informational self-determination may be restricted in certain specific cases in a necessary and proportionate manner in line with the purpose and period of processing. Based on the interest assessment test, it can be established that the processing does not constitute an unnecessary or disproportionate restriction of the rights and freedoms of the data subject. The data subject may object to the processing and may at any time exercise his rights guaranteed in Articles 12-22 of the General Data Protection Regulation at any time."

(6) In view of the above, the Authority closed the Antecedent Case on the basis of Section 55(1)(a)(ab) of the Privacy Act on 23 September 2021, and launched its current data protection procedure ex officio concerning the practice of processing related to the recording of phone calls by the phone-based customer service of the Client between 25 May 2018 and the day of launching of this procedure.

I.2. This data protection procedure by the Authority

(7) The subject matter of this data protection procedure by the Authority was the investigation into processing related to the automated analysis of the voice recordings of the incoming and outgoing calls of the Client's phone-based customer service and on that basis, listening in to a part of the voice recordings and calling back some of the data subjects in the recordings listened into. The Authority also investigated the processing of the personal data of third person data subjects calling the customer service, as well as the employee data subjects working at the phone-based customer service of the Client in relation to the above activity.

(8) Based on Section 76 of Act CL of 2016 on General Administrative Procedures (hereinafter: Administrative Procedures Act) the Authority called upon the Client to make observations and statements in relation to the current procedure, as well as the Antecedent Case to be taken into account ex officio in this procedure, and posed questions attempting to clarify the circumstance of

client identification and voice recording by the phone-based customer service on 23 September 2021.

(9) Upon the Authority's request, the Client made the following statements in its response received in an electronically signed e-mail filed under No. NAIH-7350-2/2021 received on 29 October 2021:

(i) Whenever in the course of a conversation, information related to the data subject (bank secret) would be issued, the Client always identifies the data subject requesting a unique telecode or information linked to the banking product accessible only to the data subject. In the case of an outgoing call, the data subject is called on the phone number recorded by the Client and in addition, he is identified as described above.

(ii) In the case of an outgoing call, the content of the oral information is: *"Good day to you, I am XY, calling you from the Bank, I am looking for ZW. Please be informed that our conversation is recorded for the purpose of quality assurance."*

(iii) The Client maintains its statements made in the Antecedent Case with the addition that the Software enables the individual inspection and listening in to a ranked call by clicking on it. In the course of this, the parameter of ranking is displayed in the diagram of the speech. This is needed to ensure human control because evaluation merely by the machine could lead to erroneous conclusions. (For instance, the reason for the silence is a line failure or the machine analysis erroneously assesses the tone of the voice as dissatisfied.

(iv) The Client's practice of data processing has not changed in merit since 25 May 2018, and the investigation by the Authority did not explore any circumstance that would warrant a substantial transformation of the process. The review of the practice of providing information is in progress. It is expected that as a result of the investigation, the Client will draw up information which will be more detailed at a number of points.

(v) The called party can communicate that he does not consent to the recording by discontinuing the call. If he does not do so, implicitly he gives his express consent by starting the conversation.

(vi) The technical system records from the start of the call, this cannot be influenced by the participating parties.

(vii) The system also monitors the voice of the Client's employees. In specifying the criteria of ranking, the monitoring of the voice properties of the employees can be set. This assists in the development of the employee, when necessary, without detrimental consequences in terms of labour law.

(viii) The Software does not include artificial intelligence; it does not make automated decisions. The results of its analysis can be utilised exclusively with human intervention and interpretation.

(ix) Not only customers make use of the phone-based customer service. In 2021, the monthly average number of calls was 81,500/month. Annually 1-1.5 million calls are affected by voice analysis.

(x) The Client as a financial institution pursues a large number of exceedingly complex processing operations. Relative to this, the number of data protection complaints is exceedingly low and the Client has not yet received a data protection fine.

(xi) The net sales of the Client amounted to HUF 81,002,000,000 in 2020.

II. Legal provisions applied

(10) Pursuant to Article 2(1) of the General Data Protection Regulation, this Regulation applies 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.

(11) Pursuant to Section 2(2) of the Privacy Act, the General Data Protection Regulation shall apply to data processing subject to this Regulation with the additional rules specified in the provisions therein stipulated.

(12) Pursuant to Section 60(1) of the Privacy Act, in order to ensure that the right to the protection of personal data is enforced, the Authority shall launch an authority procedure for data protection upon the application of the data subject and it may launch an authority procedure for data protection ex officio.

(13) Pursuant to Section 71(2) of the Privacy Act, the Authority may use in its other procedures the documents, data or other means of evidence lawfully obtained in the course of its procedures.

(14) Unless otherwise provided for in the General Data Protection Regulation, the provisions of the Administrative Procedures Act shall apply to the authority procedure for data protection launched upon application with the differences specified in the Privacy Act.

(15) Based on Section 4(1) of the General Data Protection Regulation, “personal data” means any information relating to an identified or an 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, physiological, genetic, mental, economic, cultural or social identity of that natural person.

(16) Pursuant to Article 4(4) of the General Data Protection Regulation, “profiling” means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

(17) Pursuant to Article 4(14) of the General Data Protection Regulation, “biometric data” means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

(18) Pursuant to Article 4(15) of the General Data Protection Regulation “data concerning health” means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or health status.

(19) Pursuant to Article 5(1)(a) of the General Data Protection Regulation, personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject (“lawfulness, fairness and transparency”).

(20) Pursuant to Article 5(1)(b) of the General Data Protection Regulation, personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (“purpose limitation”).

(21) Pursuant to Article 6(1) of the General Data Protection Regulation, the processing of personal data shall be lawful only if and to the extent that at least one of the following applies:

a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

b) processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract;

c) processing is necessary for compliance with a legal obligation to which the controller is subject;

d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

f) processing is necessary for the purposes of the legitimate interest pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject, which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the exercise of their functions.

(22) According to Article 6(4) of the General Data Protection Regulation where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law, which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:

a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;

b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;

c) the nature of the personal data, in particular where special categories of personal data are processed pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;

d) the possible consequences of the intended further processing for data subjects;

e) the existence of appropriate safeguards, which may include encryption or pseudonimisation.

(23) Pursuant to Article 9(1) of the General Data Protection Regulation, the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited, except for the special cases set forth in Article 9(2) of the General Data Protection Regulation.

(24) Pursuant to Article 12(1) of the General Data Protection Regulation, the controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including where appropriate by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

(25) Pursuant to Article 12(2) of the General Data Protection Regulation, the controller shall facilitate the exercise of data subject's rights under Articles 15 to 22.

(26) Pursuant to Article 13 of the General Data Protection Regulation:

(1) where personal data relating to the data subject are collected from the data subject, the controller shall provide the data subject with all of the following information at the time the personal data are obtained:

a) the identity and the contact details of the controller and, where applicable, of the controller's representative;

b) the contact details of the data protection officer, where applicable;

c) the purposes of the processing for which the personal data are intended, as well as the legal basis for the processing;

d) where the processing is based on Article 6(1)(f), the legitimate interests of the controller or by a third party;

e) where applicable, the recipients or categories of recipients of the personal data, if any;

f) where applicable, that the controller intends to transfer the personal data to a third country or to an international organisation, and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Articles 46 or 47 or the second subparagraph of Article 49(1), reference to appropriate or suitable safeguards and the means to obtain a copy of them, or where they have been made available.

(2) In addition to the information referred to in paragraph (1), the controller shall provide the data subject with the following additional information necessary to ensure fair and transparent processing in respect of the data subject:

a) the period for which the personal data will be stored, or if this is not possible, the criteria used to determine that period;

b) the data subject's right to request from the controller access to and rectification or erasure of his personal data, or restriction of processing concerning the data subject, or to object to processing, as well as the right to data portability;

c) where processing is based on Article 6(1) (a) or Article 9(2) (a), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

d) the right to lodge a complaint addressed to the supervisory authority;

e) whether the provision of personal data is based on legal regulation or contractual obligation, whether it is a precondition to entering into contract and whether the data subject is under an obligation to provide the personal data, and furthermore, what are the possible consequences of not providing the data.

f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4), and at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

(3) Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject with information on that other purpose prior to that further processing and with any relevant further information as referred to in paragraph (2).

(4) Paragraphs (1), (2) and (3) shall not apply if and to the extent that the data subject already possesses the information.

(27) Pursuant to Article 21(1) of the General Data Protection Regulation, the data subject has the right to object on grounds relating to his or her particular situation at any time to processing of personal data concerning him or her, which is based on Article 6(1) (e) or (f), including profiling based on those provisions. In this case, the controller may not continue the processing of the personal data, except if the controller demonstrates that processing is justified by legitimate reasons of compelling force, which override the interests, rights and freedoms of the data subject, or which relate to the establishment, exercise or defence of legal claims.

(28) Pursuant to Article 21(2) of the General Data Protection Regulation, when personal data are processed for direct marketing purposes, the data subject has the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

(29) Pursuant to Article 22(1) of the General Data Protection Regulation, the data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which would have legal effects concerning him or her or would affect him or her to a similarly significant extent.

(30) Pursuant to Article 24(1) of the General Data Protection Regulation, taking into account the nature, scope, content purposes of processing, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this regulation. Those measures shall be reviewed and updated where necessary.

(31) Pursuant to Article 25(1) of the General Data Protection Regulation, taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing, as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall both at the time of determination of the means for processing and at the time of the processing itself implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data protection principles, such as data minimisation in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this regulation and protect the rights of data subjects.

(32) Pursuant to Article 25(2) of the General Data Protection Regulation, the controller shall implement appropriate technical and organisational measures for ensuring that by default only personal data, which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

(33) A Pursuant to Article 57(1)(a) of the General Data Protection Regulation, without prejudice to other tasks set out under this regulation each supervisory authority shall on its territory monitor and enforce the application of this regulation.

(34) Pursuant to Article 58(2) of the General Data Protection Regulation, the supervisory authority, acting within its corrective powers:

a) issues a warning to the controller or processor that certain intended processing operations are likely to infringe the provisions of this Regulation;

b) reprimands the controller or processor where processing operations have infringed the provisions of this Regulation;

c) orders the controller or processor to comply with the data subject's request to exercise his or her rights pursuant to this Regulation;

d) orders the controller or processor to align processing operations with the provisions of this Regulation, where appropriate, in a specified manner and within a specific period of time;

e) orders the controller to inform the data subject about the personal data breach;

f) imposes a temporary or definitive limitation on data processing, including its ban;

g) orders the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18, and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19;
h) withdraws the certificate or orders the certification body to withdraw the certificate issued pursuant to Articles 42 and 43, or orders the certification body not to issue the certificate, if the requirements for certification are not met or no longer met;
i) imposes an administrative fine pursuant to Article 83, in addition to or instead of the measures referred to in this paragraph depending on the circumstances of each individual case; and
j) orders the suspension of data flows to a recipient in a third country or to an international organisation.

(35) Pursuant to Article 83(1) of the General Data Protection Regulation, every supervisory authority ensures that the administrative fines imposed in respect of infringements referred to Article 83(4), (5) and (6) of the General Data Protection Regulation be effective, proportionate and dissuasive in each individual case.

(36) Pursuant to Article 83(2) of the General Data Protection Regulation, administrative fines are to be imposed in addition to, or instead of, measures referred to GDPR Article 58(2)(a)-(h) and (j), depending on the circumstances of each individual case. When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine, in each individual case due regard must be given to the following:
a) 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 extent of damage sustained by them;
b) the intentional or negligent character of the infringement;
c) any action taken by the controller or processor to mitigate the damage sustained by data subjects;
d) 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 General Data Protection Regulation;
e) any relevant previous infringements by the controller or the processor;
f) the degree of cooperation with the supervisory authority in order to remedy the infringement and to mitigate its possible adverse effects;
g) the categories of personal data affected by the infringement;
h) the manner in which the infringement became known to the supervisory authority, in particular whether the infringement was notified by the controller or processor, and if so, with what degree of detail;
i) where measures referred to in Article 58(2) of the General Data Protection Regulation have previously been ordered against the controller or processor concerned with regard to the same subject matter, their compliance with those measures;
j) whether the controller or the processer adhered to approved codes of conduct pursuant to Article 40 of the General Data Protection Regulation or approved certification mechanisms pursuant to Article 42 of the General Data Protection Regulation; and
k) 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.

(37) Pursuant to Article 83(5) of the General Data Protection Regulation, infringements of the following provisions shall, in accordance with paragraph (2), be subject to administrative fines up to EUR 20,000,000, or in the case of an undertaking up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher:
a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9 of the General Data Protection Regulation;

b) the data subject's rights pursuant to Articles 12 to 22 of the General Data Protection Regulation.
c) transfer of personal data to a third country recipient or an international organisation in accordance with Articles 44 to 49 of the General Data Protection Regulation;
d) obligations under Member State law adopted on the basis of Chapter IX of the General Data Protection Regulation;
e) failure to comply with an order of a supervisory authority pursuant to Article 58(2) of the General Data Protection Regulation or a request for temporary or permanent restriction of processing or suspension of data flows, or failure to grant access in breach of Article 58(1) of GDPR.

(38) Pursuant to Section 75/A of the Privacy Act, the Authority exercises its powers specified in Article 83(2) to (6) of the General Data Protection Regulation according to the principle of proportionality, in particular by primarily issuing, in compliance with Article 58 of the General Data Protection Regulation, a warning to the controller or processor for the purpose of remedying the infringement when the provisions laid down by law or a binding legal act of the European Union on the processing of personal data are infringed for the first time.

III. The established facts of the case and the Authority's decision

III.1. Description of the processing of data relating to the analysis of voice recordings of calls made by the Client's phone-based Customer service

(**39**) The Client as a financial institution operates a phone-based customer service. In some cases, it is a legal obligation to record and retain the calls with the phone-based customer service. The current procedure of the Authority focuses on the additional processing operations on the recorded voice files, not on recording.

(**40**) Based on decision-making powers and its own statements, the controller of the processing operations related to voice analysis using the Software is the Client. The Client alone made the decision on using the Software and set forth its terms and conditions of use in its internal rules.

(**41**) Apart from a couple of second-long calls and insubstantial calls, all the calls to and from the phone-based customer service are recorded and the sound material of the call is stored in the systems of the Client.

(**42**) The recorded sound material contains the voice of the Client's employee working at its phone-based customer service as data subject, as well as the third party called by him, or the third party calling the Client's phone-based customer service and associated with him, a unique call identifier, which is uniform in every system of the Client, the calling (called) phone number, the direction, time and date of the call, the name and organisational unit of the administrator.

(**43**) Every evening, an automated program is run on the Client's voice recording server, which erases calls of below 5 seconds. In addition, using the speech signal processing based on artificial intelligence, waiting / silence / interposition, the keywords according to the specified list, and the emotional / mood state of the speaker are automatically analysed. This can be associated with a specific person, as it can be filtered out, if the Software recognised the emotions of an employee and not that of the calling party, which is the default association, which is substantiated by the Client's statement indicated in the above paragraph (4)(xi). According to the statement of the same subsection and the annex entitled "*voice képernyők.docx.doc"* technical file enclosed with the statement filed under No. NAIH-5161-5/2021, the efficiency of the system based on the recognition of emotions can be strongly questioned as the emotion was unrecognisable in 91.96% of the cases. In relation to this, the Authority underlines that the personal data becomes personal data not because

of its accuracy, but because of its association with a specific person. For instance, the storage of an unreal age which was incorrectly recorded and stored linked to an identifiable data subject will be the processing of personal data by the given controller as if the data was accurate.

(**44**) The analysis, use and storage of the voice and emotional / mood state of data subjects qualifies as the processing of sensitive data. Although according to the assessment of the Authority, the specific case is not about the special category personal data according to Article 9(1) of the General Data Protection Regulation, irrespective of this, their processing concerns the privacy of the data subjects.

(**45**) As to whether the data generated in the course of the processing under investigation qualify as special category personal data according to Article 9(1) of the General Data Protection Regulation based on all the circumstances of this case, the Authority established the following. Of the data constituting the results of voice analysis, only the emotional psychological status is the one which may qualify as biometric data or health-related data under the given circumstances. In this case, according to the explored facts of the case, the voice analysis generates data, which do not uniquely identify the data subject, thus this condition of biometric data is absent. As to the health-related data, there is a condition that does not obtain, namely that conclusions of merit could be drawn from the result of the processing constituting the subject matter of this case as to the physical or mental health condition of the data subject. Irrespective of this, the conditions do not obtain, not because of the applied method or the quality of the data itself, so in a given case under identical conditions in other cases, similar data could qualify as special category personal data, if the other circumstances based on connection to other data – which did not take place in this case – meet the above conditions.

(**46**) Based on the above, the Software evaluates the performance of the Client's call centre employee by analysing the waiting times/silence/parallel speech, on the basis of which senior employees may call for individual development, training in specific areas or process improvement according to the Client's statement referred to in Section 2 (xiv) above in Section 4 (i) above, which may also affect the performance pay of the Client's call centre employees.

(**47**) The Software also stores the result of the recognised keywords and emotions per call linked to the given call, and the calls can be replayed within the voice analytics Software for up to 45 days, but are retained in the voice recording system beyond that time. In this context, the content of the privacy notice referred to in Section 3(iii) above only refers back to Section 3.1.8 of the General Terms and Conditions of Business, which lists different retention periods for several data processing operations for different purposes, and it is unclear and non-transparent for an average data subject.

(**48**) The Software ranks the calls based on the above, which is a suggestion as to which person should be called back first, which complainant is more dissatisfied. This data, which describes the emotional and psychological state of the data subject at the time of the call based on the Software's analysis, is also stored in the Software in connection with the call. Based on this information, the Client's senior employees can decide who to call back by the Customer Service to address the dissatisfaction. The Software is not designed to handle individual complaints, but all complaints reported by telephone are handled in some way by the customer service staff, regardless of the functioning of the Software. The purpose of the call-back is not to address the specific complaint, but to filter and address the customer's remaining dissatisfaction regardless of the resolution of the specific complaint in principle.

(**49**) Based on the Client's statements in the Antecedent Case as indicated in Section 2(iii), (iv) and (v) above, the purpose of the processing is to monitor the quality of calls based on variable parameters, to prevent complaints and customer churn, and to increase the efficiency of the staff handling the calls. The Privacy Notice provided to data subjects on the Client's website, as referred

to in Section 3(iii) above, is very general about this processing, the words *"performs profiling based on legitimate interest and selects calls by automatic decision-making in which a more highly qualified bank employee resolves the problem or complaint raised in the call by means of call-back"* do not communicate the substantive method and essence of voice analysis and are not clear. Furthermore, the information only refers to quality assurance and complaint prevention as purposes, but the above description, which does not provide any substantive information, also refers only to complaint prevention. Therefore, data subjects are clearly not aware of the existence of the processing, its material content and all its purposes, and they do not receive this information when making the call or when they are called back.

(**50**) The Client has based the above processing on its legitimate interests in order to retain its customers and to improve the efficiency of its internal operations. However, the processing of these interests, which are very different, were not separated in the minimal information notice or in the interest assessment and the Client did not address them separately.

(**51**) Although it is not the subject of the present proceedings, the Authority records as a fact that the registration of the processing in question would not have been automatic due to the application of the new processing technology, pursuant to Section 68(4) of the Privacy Act in force before the General Data Protection Regulation became applicable, when the processing started. In such cases, the conditions and guarantees of the processing are qualified individually by the Authority at the request of the Client, and the Client could not have started the processing without the prior approval of the Authority. As this approval procedure was not carried out through the fault of the Client, the Authority became aware of this processing with a significant delay. Moreover, the records of the processing of the sound recordings within the meaning of GDPR Article 30, as referred to in Section 3(vi) above, which the Client has sent to the Authority, do not mention any processing of the sound recording, but only its storage.

III.2. Application of the General Data Protection Regulation to the processing of data by the Software

(52) According to GDPR Article 4(1), even indirect identifiability is sufficient to qualify as 'personal data'.

(53) Pursuant to GDPR Articles 57(1)(a), 58(2)(b) and (d), 83(1), (2) and (5) and Section 75/A of the Privacy Act, the Authority examined ex officio the part of the Client's general practice in its procedure that is relevant to the present case. The Authority may use documents and evidence lawfully obtained in any other proceedings pursuant to Section 71(2) of the Privacy Act in other proceedings.

(54) The Client stated in its reply letter in the Antecedent Case, registered under File No. NAIH-5161-5/2021 received on 5 July 2021, that in its opinion the Software does not store any identifying data, and the results of the analysis produced by the Software on the emotional state of the caller and the customer service employee are not personal data, because they cannot be linked to anyone, and compared the system to the operation of traffic counters and traffic lights. This is clearly in conflict with the information provided by the Client in its reply letter in the Antecedent Case, filed on 16 August 2021 under File No. NAIH-5161-10/2021, that customer service calls are assigned a unique internal identification number that can be linked to the caller and the customer service employee outside the Software but within the Client's systems, and that this unique identifier is also used as a pseudonym by the Software. When a consequence is applied (e.g. call back, sending for training), this linkage is established. A traffic counter or a traffic light cannot be used to subsequently re-identify, for example, the fourth car that has passed in front of it and call the driver. The Software does not work on this principle at all, but is explicitly designed to operate in order to take measures specific to data subjects.

(55) Based on the above, both parties to the call can be clearly identified by the Client, which the Client actually does throughout the normal operation of the system in relation to those whose recorded calls are listened to and then, where appropriate, are called back or the call centre employee is evaluated on this basis. If the Client does not do so, but has the possibility to do so, the result of the analysis by the Software would still be personal data until the relationship with the relevant identifiable data subjects is irreversibly terminated.

(56) The above interpretation is confirmed, inter alia, by the judgment of the Court of Justice of the European Union in Case C-582/14 in relation to dynamic IP addresses, which is analogous to the present case, and which are also personal data in relation to all data controllers who have access by lawful means, including indirectly by transmission to public authorities, to information from an ISP about the subscriber to whom an IP address belongs at a given time. In the present case, the necessary identifying information – linking the pseudonymous identification number with the telephone number and other call data – is available to the Client within its own systems, so there can be no question that it had lawful means to do so. It is important to underline that the concept of lawful means, as indicated by the Court, does not refer to the lawfulness of the processing or compliance with data protection rules, but to the fact that the means used are not in themselves unlawful (such as a black-market database is an unlawful means regardless of the processing for which it is intended). Unlawful means cannot, in principle, be used to carry out lawful processing, but lawful means may be used to carry out lawful or unlawful processing depending on the other conditions, including purpose, legal basis, etc. In the absence of identifiability, the results of the analysis would clearly not allow the customer service to know who to call back, nor could the customer service employees be checked in the same way as they are on the basis of the Client’s own statements.

(57) Although the Authority's investigation focused on the operation of the Software, the nature of personal data in such a complex processing is not determined by whether the data subject can be identified within a subsystem. It is necessary to examine all data sources lawfully available to the Client to determine whether the condition of direct or indirect identifiability applies. Pseudonymisation (use of pseudonymous identifiers) is a data security enhancing circumstance, but does not affect the unique identifier and the quality of personal data for third party callers. The personal data nature with respect to the Client's call centre employees should not even be an issue, as their names are also stored in relation to the result of the analysis of a particular voice recording, which is linked to a particular voice recording. With regard to third party data subjects, GDPR Article 4(1) treats indirect identifiability in the same way as direct identifiability, and GDPR Article 4(5) also considers pseudonymous identifiers themselves as personal data, including other information stored in connection with them, if the identifier itself can be linked to a specific natural person. And a telephone call does not exist in itself, there is a natural person behind it. At the beginning of a telephone call, the Client’s Customer Service always identifies the data subject to whom it is speaking, so both the recordings heard and potentially heard contain the identification data. The fact that the Client has been able to establish, by its own declaration, that in some cases the emotion identified was that of its own employee also confirms the possibility of unique identifiability.

(58) Based on the above, the emotional state recognized by the Software, the length of silence and the data related to the caller ID and telephone number used in the Software are considered personal data, regardless of their encryption or pseudonymization, as long as they can be linked to individuals, even if through other data legally available to the Client. In the case of listening to the recording, the first audible data on the audio recording is always the identification of the speaker, so not even pseudonymisation exists at this point of processing for recordings heard. This is regardless of whether the connection is made by the Client in the specific case, it is sufficient if there are lawful means at its

disposal.[1] The fact that, for example, conclusions are drawn from the length of silence primarily not about the caller but about the work of the customer service agent – which may or may not prove correct in the course of human verification – still constitutes the personal data of that agent for the time of processing. The fact that a piece of data subsequently proves to be incorrect or inaccurate does not cast doubt on its personal data character, since any data – not only real data – linked to a specific natural person constitute personal data.

(59) On the basis of the above, the provisions of the General Data Protection Regulation apply in principle to the processing of data using the Software and there are no contrary circumstances in the present case.

III.3. The use of Artificial Intelligence in the Software

(60) In its reply letter received on 29 October 2021, registered under File No. NAIH-7350-2/2021, the Client stated that *"the Software does not contain artificial intelligence, it does not make automated decisions, and its analysis results can only be used with human intervention and interpretation*".

(61) After examining the information available on the Software through a public search of the Internet, the website of the company that developed the Software, the questions posed by the Authority and the answers given to them, the Authority has concluded the following. The company that develops the Software is a Hungarian company that markets its products in several countries. According to the description available on the company's website*, "it is a company active in the field of artificial intelligence and predictive analytics solutions, software development and consulting in connection with customer service activities, operations, project and HR management. […]."*[2]

(62) The company's Hungarian language website above prominently features an application called the Voice Analytics Platform (the "Platform"), which is the basis of the Software's operation, and is described on the website by its developer as follows: *"The Platform is a comprehensive performance and quality management solution for customer services based on speech and data analytics. The application analyses customer service conversations from both the customer's and operator's side, recognising the words spoken, angry, dissatisfied, disappointed, uncertain, neutral or satisfied moods, as well as other factors that affect the quality of customer service and performance, such as silence, music, speech rate, volume, speech quality and intonation, and other quality characteristics. By processing all conversations, the system provides a complete insight into the elements that have a decisive influence on the quality and performance indicators of customer services. Get the most out of your customer service, reduce your average call time, increase your performance and improve the quality of customer service, all at the same time. In addition to having advanced business intelligence-based analytics, make it more active, automated and efficient."*

(63) According to a description on the Platform's English-language information page, the Platform uses machine learning and artificial intelligence to identify and measure emotions, keywords and phrase-based emotional and speech characteristics such as speech rate, inflection and articulation based on speaking style. The page also states from the developer of the product that a carefully trained neural network sorts the voice fragments into three main categories[3]

---

[1] See, by analogy, judgment of the Court of Justice of the European Union in Case C-582/14, paragraph 49.: *„[…] a dynamic IP address registered by an online media services provider when a person accesses a website that the provider makes accessible to the public constitutes personal data within the meaning of that provision, in relation to that provider, where the latter has the legal means which enable it to identify the data subject with additional data which the internet service provider has about that person."*

[2] […]

[3] *„An extensively trained deep neural network classifies speech segments into three main categories […]"*

(64) As indicated in the descriptions referred to, the Platform covers topics of artificial intelligence, machine learning and neural networks.

(65) Artificial intelligence is the development of computers and robots in ways that allow them to operate in ways that can mimic or exceed human capabilities. Programs using artificial intelligence can analyse and put into context data to provide information or automatically trigger certain events without human intervention[4].

(66) Machine learning is one of the possible paths to artificial intelligence, in fact one of its tools. In this sub-field of artificial intelligence, algorithms are used in such a way that they learn to automatically recognise patterns and relationships in the data, and then apply what they learn to make (or suggest) increasingly better decisions.[5]

(67) Neural networks are a possible approach to machine learning that builds on a simplified scheme of human brain function to resolve problems that ordinary algorithms cannot handle.[6] A neural network consists of simple units – neurons – every one of which, like real neurons, receives inputs and sums them up to produce outputs. However, the incoming signals are not taken into account to the same extent by each neuron to determine the output value, but are weighted, to use the statistical term. The reason for this can be best illustrated by an example: if a neural network is used to estimate (predict) property prices in a specific case, the district of Budapest and the comfort level of a property are not as important as whether it is on the 3rd or 4th floor. It is important to note that neurons, although they perform calculations, are not processors. The main difference between the two is that while processors are programmed, i.e. they are given an essentially fixed sequence of instructions to be executed one after the other, which cannot be modified by themselves and always have predetermined output values, neurons are trained by adjusting the values of the weights, so that they can give a value unknown to the user of the algorithm, depending on the algorithm used[7].

(68) According to the specifications referred to above, it is the developer himself who provides the information about the parameters that the Platform as a software product is capable of identifying and evaluating, and the IT methods and solutions used for this purpose, which belong to the realm of artificial intelligence.

(69) The Software is capable of automatically evaluating calls received and initiated by call centre staff based on predefined rules, such as the "greeting rule", which checks whether the staff member has greeted the customer properly, or the "inquiry rule", which allows the system to check whether

---

[4] See: https://ai.engineering.columbia.edu/ai-vs-machine-learning/ *„Artificial Intelligence is the field of developing computers and robots that are capable of behaving in ways that both mimic and go beyond human capabilities. AI-enabled programs can analyse and contextualize data to provide information or automatically trigger actions without human interference."; this approach is reinforced, inter alia, by the European Union's legislative proposal currently in draft form: https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52021PC0206*

[5] See: https://ai.engineering.columbia.edu/ai-vs-machine-learning/ *„Machine learning is a pathway to artificial intelligence. This subcategory of AI uses algorithms to automatically learn insights and recognize patterns from data, applying that learning to make increasingly better decisions."*

[6] See in greater detail: Report by the Council of the European Union on Artificial Intelligence, its main capabilities and scientific methods; Published on 8 April 2019; URL: https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines

[7] See in greater detail: Tamás Klein: Robotjog, vagy emberjog? In: „A mesterséges intelligencia szabályozási kihívásai", Budapest, 2021, p. 129, see also „A Closer Look at Neural Networks"; published on 02.08.2019.08.02.; URL: https://docs.microsoft.com/en-us/archive/msdn-magazine/2019/february/artificially-intelligent-a-closer-look-at-neural-networks

the staff member has tried to collect the necessary information from the customer by asking the necessary number of questions.[8]

(70) Within the context of the automatic evaluation of the performance of employees working at the call centre, the system is also able to measure the time that elapses between asking a question and answering it during a call (the so-called "silence period"), which can be used to draw clear conclusions about the employee's level of knowledge and skills.[9]

(71) On the basis of the above, it can be stated that the Software uses artificial intelligence to automatically process personal data, resulting, on the one hand, in a list of calls in the order in which they are to be returned, and, on the other hand, the recognised emotions and voice recording characteristics associated with each call (e.g. the length of pauses), until their deletion, which, according to the Client's statements in the Antecedent Case, is 45 days. It is not a prerequisite for automatic data processing that the decision should be made by the machine, it is sufficient if it is intended to produce a result that influences the decision makers, it is taken into account in the human decision that is made here. This is confirmed by the document attached to the reply letter received from the Client in the Antecedent Case on 5 July 2021, filed under File No. NAIH-5161-5/2021, which is called an Interest Assessment, but is in fact a Privacy Impact Assessment document, as the file name suggests (identifier: "*„érdekmérlegelési teszt voicemining.xlsx* "), which states that *"The data processing is high risk for several reasons, with particular regard to the novelty of the technology used, as the voice recordings are analysed and findings are made automatically using artificial intelligence. The totality of the data is suitable for profiling or scoring for both sets of data subjects and, although no automated decision making is involved, the data processing may have legal effects on the data subjects."*

(72) For the reasons explained above, **GDPR Article 21 applies** to the processing of data through the Software. In addition, **profiling within the meaning of GDPR Article 4(4)** also take place, as the data generated by the system will also be used to monitor and evaluate the performance of the Client's call centre employees at work, due to the core functionality of the system, as set out in the Customer Declaration referred to in Section 4(i) and the online source referred to in paragraph 66. Also, profiling is supported by the prioritisation of dissatisfied customers for recall based on keywords and emotions, a feature that corresponds to the assessment of a personal characteristic under GDPR Article 4(4). The term profiling is also used in the Client's internal note on customer complaint [...] described in Section 3(i) above and in the privacy notice described in Section 3(iii)(c) above. The data processing is based on the technology for analysing the emotions of natural persons, which is a new technology. This, contrary to the statements made by the Client in the course of the procedure, in fact creates increased risks to fundamental rights, and therefore, in accordance with the risk-based approach under GDPR Articles 24 and 25, the Client's responsibility as controller in this respect is also increased.

III.4. Lack of adequate information and the absence of the right to object

(73) No information is given to data subjects orally at the beginning of the conversation about voice analysis and the automatic analysis and evaluation of their emotions and the resulting possibility of a callback.

(74) The only information provided by the Client to the data subjects referring to the data processing with the Software, but not containing any specific information, is this sentence of the "Detailed information on data processing in the phone-based customer service and complaint management",

[8] […]
[9] […]

according to which data subjects are not given any information about the specific types of data, only that *"For quality assurance and complaint prevention purposes, the phone-based customer service performs profiling based on legitimate interest and selects by automatic decision the calls in which a more highly qualified bank employee resolves the problem or complaint raised in the telephone conversation by means of a callback."* Beyond this, data subjects are not given any information at all about which specific types of their data are processed in what way and how their emotional reactions are evaluated. Apart from the legal basis, all information that would be otherwise mandatory pursuant to GDPR Article 13 is missing, and the purpose indication is incomplete. The duration of processing is not clearly indicated in a way understandable for an average data subject either in the "Detailed information on data processing for phone-based customer service and complaint management" or in Section 3.1.8 of the General Rules of Business.

(75) The purpose stated in the above information is to provide quality assurance and prevent complaints. Neither the prevention of customer churn, nor the improvement of internal efficiency are among the purposes indicated to data subjects.

(76) The Client's statements set out in Sections 4(vii) and (viii) of the justification above also confirm the above, in that the Client is aware that it has not provided adequately transparent and concise information and the right to object for years in connection with the processing of the voice analysis under review, due to the particular difficulty of the latter. This is contrary to the Client's privacy statement, which states that it guarantees the rights of data subjects. In its interest assessment, the Client has, inter alia, invoked the adequate safeguarding of data subjects' rights to classify the processing as risk-free and free from any infringement, without justification for a number of reasons.

(77) The right to object on the basis of legitimate interest and the right to object to automated processing is not at the controller's discretion; it is the Client who must ensure these rights under GDPR Article 21. In any event, the complete absence of the right to object in the present case leads fundamentally to a breach of GDPR Article 21, but the Authority establishes in principle that phone-based solicitation for customer retention purposes constitutes a marketing purpose similar to customer acquisition, and therefore an objective right to object under GDPR Article 21(2) should be granted to data subjects in this context, while for other purposes – quality control, internal efficiency gains – a conditional right to object under GDPR Article 21(1) should be granted. This is one of the reasons why it is not appropriate to mix and combine the different purposes of processing and interest assessments of the controller, since the end result – and the conditions to be fulfilled to achieve the appropriate end result – may not be the same for each purpose.

(78) Although the Client did not indicate consent as the legal basis, it also invoked it. In this respect, the Authority notes that, according to the General Data Protection Regulation, only informed consent, freely and actively given, could be the basis for processing, which is excluded as a legal consequence of refusal of the service (phone-based customer service). The same is true for employees, in a relationship of subordination, the use of this legal basis is in principle excluded, as complete freedom from influence in the performance of their work is not conceivable. It is also fundamentally flawed and unacceptable for the Client to argue that no complaints have been received from data subjects about the processing under review, when the data subjects could not have been informed of it in any meaningful way.

(79) On the basis of the foregoing, data processing by the Client in relation to the analysis activities of the Client's customer service voice recording **is in breach of GDPR Articles 5(1)(a) and (b), 12(1), 13, 21(1) and (2)** in its current form.

III.5. Qualification of the interest assessment in relation to data processing by the Software

(80) The operating principle of AI, as explained in Section III.3 above, is generally difficult to understand and follow. This is one of the reasons why the use of artificial intelligence in data processing requires particular care – not only in its description on paper, but also in its actual implementation – if the controller wants to comply with the transparency and accountability requirements of the General Data Protection Regulation. This goes beyond the default level of expectation for data processing at normal risk and, taking into account the risk-based approach under GDPR Articles 24 and 25, this difficulty should be taken into account when the controller decides when and for what purpose to use AI and how to ensure transparency in this respect.

(81) The effectiveness of the emotion analysis and satisfaction evaluation and recording system used in the Software is relatively low, based on the technical annexes submitted by the Client in the Antecedent Case (identifier: *"voice screens.docx.doc"*). This also does not confirm that voice analysis in its current form is suitable to achieve the stated objectives and that its use in its current form would represent an unavoidable and proportionate restriction of the rights of data subjects, even if, unlike in the present case, the rights of data subjects were adequately safeguarded by the Client. The Client's interest assessment did not take this into account in any way, no information about the timing or review of the interest assessment is evidenced by any documents provided by the Client, nor does the interest assessment indicate that any periodic review was scheduled to verify that the actual operation of the Software is adequate and that it adequately protects the rights of data subjects.

(82) The voice analysis activities carried out by the Client using artificial intelligence, in particular the evaluation of the emotions of the data subjects, raise in themselves data protection issues of principle. Years ago, in its 2012 Annual Report, the Authority already stated that: *„It is typical for the financial sector to be at the forefront of using new data processing technologies. The analysis of the audio recordings of conversations with the bank's customer service can provide hidden information that can be used to make conclusions about the customer's willingness and ability to pay. However, when using tools to examine psycholinguistic features and the emotional tones of speech it is not sufficient to assess the formal existence of the person's consent. The prioritisation technology based on speech processing means an invasion of privacy and carries risks that the data subject is not able to recognise at the time of giving consent and to assess the impact on his personal rights. The Authority has pointed out that data mining technology allows the financial institution to obtain data of which the customer is not even aware, so that the use of such tools reduces the data subject from being the subject of the procedure to being the object of it."*[10] This also underlines the importance of the choice of the data processing method and the guarantees and data subjects' rights when using artificial intelligence. Pseudonymisation – the use of an internal voice recording identifier – is generally useful, but is not in itself, especially in the present case, a sufficient guarantee.

(83) Joint Opinion 5/2021 by the European Data Protection Board and the European Data Protection Supervisor on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) contains the following statement: *" Furthermore, the EDPB and the EDPS consider that the use of AI to infer emotions of a natural person is highly undesirable and should be prohibited, except for certain well-specified use-cases, namely for health or research purposes (e.g., patients where emotion recognition is important), always with appropriate safeguards in place and of course, subject to all other data protection conditions and limits including purpose limitation."*[11]

(84) In addition to the above, based on the facts disclosed and the statements of the Client set forth in Section 4(vii) and (viii) of the justification above, neither adequate prior information, nor objection

[10] https://www.naih.hu/eves-beszamolok?download=17:naih-beszamolo-2012-februar
[11] See para 35: https://edpb.europa.eu/system/files/2021-10/edpb-edps_joint_opinion_ai_regulation_hu.pdf

is ensured for the specific method of processing, and the rights of data subjects are therefore completely annulled by the Client's practice of analysing recordings made by means of phone-based voice recording.

(85) The interest assessment was not done separately for each purpose, but all purposes were merged into one data processing. The issue should have been to establish adequacy and proportionality for the given purpose of processing; instead, the Client's assessment was based solely on its own interests, whether perceived or real, as to whether the processing was necessary and proportionate to achieve the purpose of the processing, and even this was done on a formal basis. The Client has only established that the processing is necessary for the purposes of the interest it seeks to achieve, and it has not compared the impact of its activities for each purpose with the rights of the data subject. It did not actually consider proportionality and the data subject's side, belittling the significant risks to fundamental rights. In particular, it failed to take into account the guarantee effect of the right to adequate information and the right to object, i.e. the rights which in reality are not granted to data subjects by the very design of the system, thus completely removing the right of self-determination of data subjects. Thus, the result of the interest assessment, as explained above, is fundamentally flawed and misleading on the question of adequacy and proportionality, and it does not even compare what it should be comparing. The fact that the Client should be performing its tasks by employing fewer customer service staff is not in itself a proportionate and adequate justification for the removal of the fundamental rights of data subjects and for the use of a form of data processing that the Authority and the EDPS consider undesirable and involving high risk, even if adequate data subject rights are ensured. Innovation only benefits people if it is appropriate, effective and accompanied by strong safeguards. Instead of enhanced guarantees, the Client has demonstrated the opposite in the clarification of the facts of the case in relation to voice analysis.

(86) Unjustified or erroneous planning and assessment of the processing does not constitute an unavoidable cause beyond the Client's control; it is solely an intentional act of the Client, who started or continued the processing knowing that it was fundamentally flawed and not actually supported by the interest assessment, but only by the paper trail. The Client failed to prove that it actually considered any alternatives. Voice recording is an unavoidable element of running a phone-based customer service, due to a legal obligation in the case of complaints, otherwise at the Client's discretion, and it is a significant injury to the interests if the call centre is unavailable to someone who does not wish to accept all the data processing associated with it, which is not even fully knowable. If the Client wishes to carry out further processing operations with the mandatory voice recordings, to analyse them in an automated manner using new and not fully known, risky technologies, he must also comply with GDPR Article 6(4), since it wishes to process personal data for a purpose other than the purpose for which the data were collected. In such a case, the controller must investigate whether the data subjects can reasonably expect processing to happen and whether the new processing is compatible with the original purpose – in the current case the recording of conversations for the fulfilment of a legal obligation – before the processing starts and appropriate safeguards must be in place at all times. The analysis of an audio recording available for a completely different reason, without the knowledge and choice of the data subject, cannot be lawful from a data protection point of view if the data subject could not have been informed about it and the data subject's rights are not guaranteed, which the Client, despite being aware of it, did not take into account afterwards and it continued the processing, knowing all of this. This justifies the intentional nature of the infringement.

(**87**) At the discretion of the Client, the voice of its employees is also analysed and evaluated and used, inter alia, for performance pay purposes, based on the Client's statement under Section 4(i) above. In the case of the employee data subjects, it is also questionable what actual chance they would have to object on the grounds of subordination. This circumstance has also not been

considered by the Client. With regard to employees, monitoring the performance of the contract and quality assurance may – also as a result of labour law rules – give rise to certain legitimate interests under certain circumstances. However, in this case, the question of suitability and proportionality is also of paramount importance, which is called into question, inter alia, by the Client's own statement under Section 4(xi) above, and an adequate system of guarantees is not provided for employees who are in a subordinated relationship and are therefore more vulnerable than third parties. The analysis of emotions, the effectiveness of which remains unproven and profoundly and severely limits their right to self-determination, cannot be supported in a reasonable manner in the case of the employees. Since employees are also explicitly subject to workplace performance-related profiling under GDPR Article 4(4), a thorough analysis of the rules and safeguards applicable to this is also necessary before processing data with a new technology, which the Client has also not done in its interest assessment.

(88) Also, the Authority does not share the Client's view that the data subjects do not sustain any harm in connection with the processing under investigation. The General Data Protection Regulation serves to protect the right to the protection of personal data, which is considered a fundamental constitutional right under Article VI(3) of the Fundamental Law and Article 8(1) of the Charter of Fundamental Rights of the European Union. Any unnecessary restriction or denial of the data subject's rights to the protection of fundamental rights, as laid down in the relevant legislation, in particular in Chapter III of the General Data Protection Regulation, results in a significant breach of fundamental rights, even without direct financial loss, and this is the case for a large number of data subjects. According to the Client's statement, this amounts to the processing of approximately 1 to 1.5 million voice recordings per year.

(89) The Authority has also considered the applicability of GDPR Article 22(1) to the processing at issue in the present case, as it also affects the data subjects' rights to be provided by the Client. The Client also failed to do so when designing the processing. A decision based on fully automated processing is implemented in the present case for data subjects who are not selected to be called back or no administrative error is reported, so in these cases a negative decision is made without human intervention. In the case of employees, performance evaluation also takes place. Nevertheless, in the present case, the Authority found that the condition of GDPR Article 22(1) that there is a legal effect or a similarly significant impact on the data subjects of a decision based on fully automated processing is not fulfilled in the case of a negative decision, since in their case there is no reaction whatsoever. Human intervention is required to take further action in the case of persons selected by the Software to be called back or of employees to be reviewed, so for these persons a significant impact is achieved, but the condition for a decision based on fully automated processing is not met. Therefore, on the basis of all the circumstances of the present case, the Authority has established neither the applicability of GDPR Article 22(1), nor a breach thereof. However, in the case of extensive automated processing, the failure of the controller to consider this possibility on the merits, as the Client failed to do in the present case, demonstrates a shortcoming of the interest assessment.

(90) As set out in this section, the interest assessment done by the Client does not provide a fair result based on the analysis required by the General Data Protection Regulation, and therefore the priority of legitimate interest based on it over the rights and freedoms of the data subjects cannot be established in the context of the processing in question.

III.6. Lawfulness of data processing using the Software

(91) Due to the invalidity of the assessment of interests, the Authority considers that there is no legal basis under GDPR Article 6(1)(f) or any other legal basis listed in GDPR Article 6(1) for the automatic analysis of the audio recordings in the manner as done by the Customer.

(92) The Client has not provided any guarantees or substantive rights of objection in relation to third party data subjects so, in this respect, the analysis of objective factors (words, pauses) other than emotions is only possible if this activity is carried out with appropriate guarantees, on the basis of appropriate proportionality and the necessity assessment. If the Client wishes to carry out an analysis of factors other than emotions, which can be precisely indicated in the information, it may only do so subject to the guarantees provided for in the General Data Protection Regulation and not without limitation. One of the major challenges of AI is the issue of ensuring transparency, which in this case has failed completely with regard to the data subjects[12].

(93) In relation to its employees, the Client is better able to base its analysis on objective factors (words, pauses) other than emotions than in the case of third parties, since, in certain circumstances, the analysis of customer service voice recordings may be necessary to verify the duties involved in a customer service job, unlike the management of a bank account. In the case of employees, information is also easier to obtain than in the case of a third party calling in, who may not yet have any legal relationship with the Client. However, the use of this new and highly risky technology – as highlighted, inter alia, in Hungary's Artificial Intelligence Strategy – can only be implemented with very strong guarantees and proper planning, in a reliable and human-focused way. The erosion of data subjects' rights should not be the aim or the result of development. Identifying the amount and type of data that is proportionate to the purpose requires a more thorough and verifiable justification when designing data processing. If a controller uses innovative and less known and regulated technologies, expectations are higher than for classical technologies, so that increased safeguards and careful planning should also apply to the oversight of employees. This form of monitoring and profiling, in particular the analysis of employees' emotions, raises a number of legal and ethical issues that have not been identified and addressed by the Client in the course of processing.

(94) On the basis of the above, the Client's data processing practices in relation to the automated analysis of voice recordings by customer service, as described above, **violate GDPR Articles 5(1)(a), 6(1) and 6(4).**

III.7. Systemic infringement of data subjects' rights

(95) Pursuant to GDPR Article 12(1), the Client must provide the data subjects with the minimum information necessary to understand the processing in a concise and comprehensible manner, so that the data subjects are at least aware of the basic nature of the processing. This is not provided by the Client either in advance or during the returned call, and data subjects who call its customer service cannot in any way suspect that their voice is analysed automatically, and cannot reasonably expect to be called back without request, inter alia, because of the tone of their voice. In accordance with GDPR Article 24(1), the novel nature of the processing, the sensitive nature of the analysis of emotions and other psycholinguistic analyses, and the other processing circumstances identified above, should have obliged the Client to design the processing in a way that would maximise the rights and freedoms of the data subjects, which it clearly did not do. The fact that there have been few complaints from data subjects about this so far does not confirm that data subjects were not

[12] See para 72: EDPB-EDPS Joint Opinion 5/2021

upset, but that they could not reasonably have been aware of it, which in itself raises strong questions about data protection compliance.

(95) Pursuant to GDPR Article 12(2), the Client is obliged to facilitate the exercise of the data subject's rights. The right to object is a fundamental safeguard, the absence of which, regardless of any other circumstance, could in itself have rendered the finding of overriding legitimate interest unsuccessful. The existence of a legitimate interest is insufficient; it must, where appropriate, prevail over the rights of the data subject, which in the present case clearly cannot exist in the absolute absence of all the appropriate safeguards. In view of the fact that providing the rights of the data subjects is a matter within the discretion of the Client and is manifestly factually incorrect, this cannot be considered a negligent error, only a deliberate departure from the facts and a deliberate disregard of the practical application of the theory described in the assessment can be allowed to continue for years without any substantive review.

(96) According to GDPR Article 25(1) and (2), the Client should have been obliged to assess, before starting the automated voice analysis using artificial intelligence, whether the processing is feasible under the current technical and social circumstances, while ensuring maximum compliance with data protection rules. The Client's interest assessment is contrary to the statements in paragraph 4(vii) and (viii) of the above justification and the facts established support the unlawful situation. The Client knew, or with due care and diligence should have known, before the processing started, the ways in which it would or would not be possible to inform the data subjects and to enforce their rights of objection and their other rights as data subjects. On the basis of the above and GDPR Articles 24 and 25, the Client ab ovo could not have decided to start the processing based on the voice analysis in this way.

(97) The Client implemented the Software before the General Data Protection Regulation became applicable in 2017. It is unclear from the text of the impact assessment and the interest assessment when they were done by the Client and whether they have been reviewed at any time. Reference to the General Data Protection Regulation itself does not indicate a specific date of preparation. The form of the impact assessment is appropriate, but its content, as explained in the present Decision, does not correspond to reality, it does not address the issue of the analysis of emotions in a meaningful way, and these shortcomings were clearly known to the Client at the time of the preparation of the impact assessment and at the time of the periodic review required during the operation, including the review following the introduction of the General Data Protection Regulation. This is confirmed by the statements of the Client presented in this Decision.

(98) The appropriate information regime in GDPR is designed to ensure that the data subject is aware of which personal data will be processed, by which controller and for what purposes. This is essential for him to be in a position to exercise his rights as a data subject in a meaningful way. In the case of processing based on GDPR Article 6(1)(f), there is an enhanced information requirement under GDPR Recital (47) . Accordingly, in addition to the specific information referred to in GDPR Article 13, it is an additional condition, inter alia, that the reasonable expectation of the data subject must extend to the processing in question, and he must expect the processing to take place. In the absence of adequate information, the data subject is by definition not in a position to exercise his data subject’s rights properly, in particular if he does not have an effective possibility to exercise the substantive right to object. As explained above, the information obligation is not a mere administrative obligation to produce a 'paper trail' under GDPR. The production of a document is not in itself a fulfilment of the controller's obligations, it should only be a means, a record, of preparing and deciding on the merits, of taking decisions and reviewing them at necessary intervals. The use of a new type of technology with increased risks also implies an increased expectation of regular and meaningful review. Both the preamble and the articles of the General Data Protection Regulation require the achievement of results when defining the obligations of the controller, not only the

performance of a certain minimum administration by the controller. The purpose of providing the information is to put the data subject in a position to make an informed choice about the exercise of his data subject's rights. There is no substantive information available to those data subjects on the processing of data through the use of the Software or voice analysis who call the Client's customer service by telephone or who are called or called back by the Client's customer service.

(99) In relation to the legal basis of legitimate interest it is important to underline that a controller may not process personal data, anytime with reference to any reason whatsoever, based on GDPR Article 6(1)(f) just because there are no other possibilities and other legal basis cannot be applied. Though it is seemingly the most flexible legal basis, by applying it the controller undertakes substantial responsibility not only with the processing of the personal data taken *stricto sensu*, but also by undertaking to meet the other related guarantee obligations. It is not a question of "generating paperwork", but of a substantive task, which is particularly true in the case of data processing where the controller is in a position of trust and has a significant dominant position vis-à-vis the data subjects. Indeed, in the absence of appropriate safeguards, the risk of a breach of the data subject's rights is such that the only outcome of interest assessment, if done properly, can reasonably be that the legitimate interests of the third party are overridden by the rights of the data subject.

(100) It is very important for controllers to be aware that it is neither the data subject's, nor the Authority's task and responsibility in an authority procedure to identify and justify the purposes and legitimate interests of the processing instead of the controller. The purposes and the legitimate interests for which the controller intends to process personal data should be clearly justified, considered and guaranteed by the controller in a concrete manner, broken down to the level of data and purposes. These safeguards should ensure, inter alia, that the data subject is aware of the processing and can object to it before the processing takes place, since his right to object is exhausted after the processing, in particular in the case of processing for a short period of time or once only, and it is not effectively guaranteed. In the present case, as explained above, it can be concluded that the conditions of foreseeability and guarantee laid down in GDPR Recital (47) have not been met at systemic level, due to the mode of implementation chosen by the Client. The possibility of adequate information and prior objection cannot technically be excluded, but was not made possible by the solution chosen by the Client, of which the Client has been aware according to the statements made by it in the course of the procedure and presented in the statement of reasons.

(101) It is also a violation or erosion of the rights of the data subject if, in the course of processing based on legitimate interest chosen by the Client, it provides significantly worse conditions than processing based on the consent of the data subject. In the case of the data subject's consent, consent would be subject to separate grounds for refusal for each of the purposes of the processing, for example, the audio recording for the purposes of complaint handling initiated by the data subject and the subsequent analysis of the audio recording thus made. As making the audio recording is not based on the data subject's consent in the first place, but largely on a legal obligation which already significantly restricts the data subject's freedom, furthermore, taking away all the data subject's choices as to further processing based on the unilateral decision of the Client would only aggravate the already highly restrictive situation. The Client has, inter alia, deliberately disregarded this obvious fact in its assessment done on paper only, solely for its own commercial interest, which is contrary to the requirements imposed by the General Data Protection Regulation on data controllers.

(102) The systemic violation of data subjects' rights is also demonstrated by the fact that in the Antecedent Case, the Client failed to provide the Complainant with basic information on data processing in a comprehensible manner, even after the Complainant had explicitly requested it, following a single general sentence on the Client's website which raised his suspicion (see Section 3(iii)(c) above). The Client could not subsequently describe to the Complainant in a clear and

concrete manner for which purposes, which data, on what legal basis and how it was processing them in the context of the voice analysis, but made only general statements and references without specifics in its reply on the adequacy of the processing. The Client's defence that no such issue has been raised so far is not relevant, firstly because the General Data Protection Regulation does not include such an aspect among the controller's obligations and, secondly, the significant lack of information provided to data subjects to date is the main reason for the lack of interest so far. The obligation to provide information under GDPR Article 13 is not a boundless obligation, its explicit purpose is to compensate for the large information advantage of the controller, in this case the Client, vis-à-vis the data subjects with regard to its processing operations. In the case of complex processing using a new technology, this information advantage is also typically greater than in the case of processing without such characteristics, and the Client should have paid more attention to compensate for it. However, the Client did not do so, despite its legal obligation to do so. This in turn demonstrates that, in general, the system deliberately designed by the Client does not comply with the principle of data protection by design and by default.

(103) On the basis of the above, the Client's data processing practices in relation to the automated analysis of voice recordings by the Customer Service as described above **violate Articles 12(1), 24(1), 25(1) and (2) of the General Data Protection Regulation**.

III.8. Legal consequences

(104) Pursuant to GDPR Articles 58(2)(i) and 83(2), the Authority may also impose a data protection fine instead of or in addition to other measures. There was no doubt that in the case of a breach of the General Data Protection Regulation, GDPR Article 58(2)(d) required the controller to be obliged to bring its processing in line with GDPR. Due to the nature of the processing, the Authority has set a time limit of 60 days for this instead of the usual 30 days. In addition, in accordance with the established case law, the Authority – in such a case – sets out in the reasoning of the decision the criteria listed in GDPR Article 83(2) which were actually taken into account in the decision when imposing the fine.

(105) As to the question of whether or not the imposition of a data protection fine is warranted, the Authority ex officio considered all the circumstances of the case based on Article 83(2) of the General Data Protection Regulation, and Section 75/A of the Privacy Act and established that in the case of the infringement exposed in the course of the current procedure, a reprimand according to GDPR Article 58(2)(b) would be neither proportionate, nor have a restraining force, hence a fine has to be imposed. In this context, the Authority took into account, first of all, that the Client's data processing practices were essentially in total disregard of the relevant legal obligations, processing personal data without making any real effort to ensure the lawfulness of the processing, other than formal administration. In the present case, the protection of personal data – which is the task of the Authority – cannot be achieved without the imposition of a data protection fine, given the totality of the circumstances for the imposition of fines, as set out below. None of the circumstances set out in Section 75/A of the Privacy Act apply, the Client is not a small or medium-sized enterprise. The imposition of the fine serves both specific and general prevention purposes, because of which the decision is going to be published on the Authority's website.

(106) In determining the level of the data protection fine, the Authority took into account the following as mitigating circumstances:

(i) there was no direct decision-making with the Software, the result of AI was used and then adjusted by human review (DGPR Article *83(2)(a)*)

(ii) the Authority has not yet identified any data protection breach against the Client (GDPR Article *83(2)(e)*).

(107) In determining the level of the data protection fine, the Authority took into account the following as aggravating circumstances:

(i) The nature of the infringement is particularly flagrant and serious, the case is significant, and the Client has breached several provisions of the General Data Protection Regulation. The largely automated nature of the processing, the use of new technology, the social issues it raises about the challenges of the digital age and the inadequacy of the controller's response to them make the present case significant beyond an individual assessment at the level of principle. The conduct of the data protection authorities in the present case could be a determining factor for many similar data processing practices of many controllers in the future, which could have an impact on the processing of an incalculable number of personal data of millions of data subjects in Hungary. (GDPR Article *83(2)(a))*

(ii) The breach has existed for an extended period of time, starting before GDPR became applicable and continuing all the time throughout the application of GDPR and it exists even today. (GDPR Article *83(2)(a)*)

(iii) Based on the scale and market position of the Client's data processing and its activities in the financial sector, the Client is expected to be more exacting than the average data controller, with 1-1.5 million voice recordings per year subject to automated processing. (GDPR Article *83(2)(a)*)

(iv) The data processing activity was carried out using new and risky technology. The banking sector is a particularly sensitive area, and the responsibility of financial institutions towards their customers and data subjects in general is high, even compared to controllers of a similar size but operating in other areas. It is fundamentally at odds with the trust placed in the financial sector to use technology in a poorly considered way that raises significant fundamental rights issues and, in the absence of appropriate safeguards, significantly violates the rights of data subjects. (GDPR Article *83(2)(a) and (d)*)

(v) The analysis of human emotions by AI is, according to the practice and the explicit opinion of both the Authority[13], the European Data Protection Board and the EDPS, very risky and should be avoided as a general rule outside certain areas. The use of such technology requires significantly stronger safeguards and more meaningful discretion than that demonstrated by the Client on the basis of the facts disclosed. (GDPR Article *83(2)(a) and (d)*)

(vi) The interest assessment covered with paperwork, at loggerheads with the obvious facts, the gross downplaying and disregard of serious risks in the internal materials and policies of the Client, in the interest assessments, the total lack of substantive assessment of the impact on data subjects both before and during processing, the disregard of the right to information and the right to object, all demonstrate a deliberate intent to circumvent data protection rules. There must have been at least a reasonable intention to infringe, and the above cannot be done by accident. Based on its statements, the Client could have known that the processing could be problematic because of the above, but ignored these aspects deliberately in its processing decisions, based on a fictitious situation and turning a blind eye to reality. (GDPR Article *83(2)(b)*)

(vii) The Client did nothing to enforce the right to be informed and the right to object, as according to its statements it considered it unfeasible, instead of modifying the processing in

[13] See point 21 of the impact assessment list published under GDPR Article 35(4), https://www.naih.hu/hatasvizsgalati-lista

order to comply with its obligations under the General Data Protection Regulation. (GDPR Article *83(2)(c)*)

(viii) GDPR Article 24(1) requires the Client to take a risk-based approach, which it has failed to adopt in the present case. The capture of the audio recordings cannot be avoided by the data subjects, so any further use of these recordings for any other purpose in such a case must be judged even more strictly. Exclusion from the use of the phone-based customer service is the only alternative offered by the Client which is not a real choice for the data subjects, and is also questionable for the data subjects called by the Client, and most data subjects are not in a position to make a choice without adequate information, which may be traced back to a systemic problem in breach of the principle of GDPR Article 25. The use of AI without due care raises risks that are orders of magnitude higher relative to risks involved previously in automated data processing without AI, and it can only be assessed in the most rigorous way. (GDPR Article *83(2)(d)*)

(ix) The regulation governing the specific new technology is still very rudimentary and it should have been taken into account as an increased risk in the course of the assessment, and the absence of strong specific safeguards due to the lack of regulation in the specific area should have obliged the Client to apply even stronger safeguards than usual under the General Data Protection Regulation, but it did not even reach the level of average safeguards. (GDPR Article *83(2)(d)*)

(x) The guarantee effect of the pseudonymisation applied was only marginal, since in practice the calling party was always identified before the staff accessing the Software and listening to the recordings, since the recorded call always starts with the identification of the person, and this obvious circumstance, among others, was also falsely presented in the interest assessment as a guarantee that only existed on paper. (GDPR Article *83(2)(d)*)

(xi) The processing involved the recording and analysis of personal data such as the emotional state, the voice of the data subject, the use of obscene language, which affect the privacy of the data subjects more deeply than technical or contact data, and their processing requires special attention. (GDPR Article *83(2)(g)*)

(xii) The Authority only became aware of the processing carried out by the Client in the present proceedings through the notification of the Complaint in the Antecedent Case, which delay in learning about the processing was due to the Client's failure to act as detailed in Section (51) above. (GDPR Article *83(2)(h)*)

(xiii) The Client’s aggregate annual net sales totalled HUF 81,002,000,000 in 2020, so a small fine would not have any punitive or preventive effect, either individually or in general. (GDPR Article *83(2)(k)*)

(xiv) The Client has carried out the processing for the express purpose of making an indirect profit, to reduce internal costs and to achieve a profit by retaining customers, and it has unlawfully subordinated to this all the other aspects that are legally required to be taken into account. (GDPR Article *83(2)(k)*)

(108) On the basis of the above, the Authority considered the imposition of a data protection fine in the amount set out in the operative part to be proportionate and dissuasive in the light of all the circumstances of the case.

IV. Other issues

(109) Pursuant to Section 38(2) of the Privacy Act, the Authority is responsible for the oversight and facilitation of the enforcement of the right to the protection of personal data and the right to have

access to data in public interest and data accessible on the grounds of public interest and to facilitate the free flow of personal data within the European Union. Pursuant to Section 38 (2a) of the Privacy Act, for natural persons and legal entities under the jurisdiction of Hungary, the tasks and powers specified in the General Data Protection Regulation for the supervisory authority are exercised by the Authority according to the provisions of the General Data Protection Regulation and this Act. The competence of the Authority extends to the entire territory of Hungary.

(110) Pursuant to Section 112(1), Section 114(1) and Section 116(1) of the Administrative Procedures Act, legal remedy can be sought against the decision through administrative litigation.

* * *

(111) The rules of administrative court procedures are stipulated in Act I of 2017 on the Code of Administrative Court Procedures (hereinafter: Administrative Court Procedures Act). Pursuant to Section 12(1) of the Administrative Court Procedures Act, administrative litigation against the decision of the Authority is within the jurisdiction of a court and pursuant to Section 13(3)(a)(aa) the Fővárosi Törvényszék (Budapest Municipal Court) has exclusive competence for the litigation. Pursuant to Section 27(1) of the Administrative Court Procedures Act, legal representation is mandatory in administrative litigations subject to the competence of a court. Pursuant to Section 39(6) of the Administrative Court Procedures Act, the submission of a petition has no deferring effect on the administrative act entering into force.

(112) Pursuant to Section 9(1)(b) of Act CCXXII of 2015 on the General Rules for Electronic Administration and Trust Services to be applied according to Section 29(1) of the Administrative Court Procedures Act and in view of this, Section 604 of Act CXXX of 2016 on Civil Procedures, the legal representative of the client is subject to an obligation to maintain contact electronically. Section 39(1) of the Administrative Court Procedures Act specifies the time and place of submitting the petition. The information concerning the possibility of requesting a hearing is based on Section 77(1)-(2) of the Administrative Court Procedures Act.

(113) Section 45/A(1) of Act XCIII of 1990 on Levies (hereinafter: Levies Act) determines the amount of the levy on administrative litigation. A party initiating the procedure is exempted from the payment of the levy in advance based on Section 59(1) and Section 62(1)(h) of the Levies Act.

(114) If the Client fails to verify meeting of the prescribed obligations, the Authority shall deem that the obligation was not complied with when due. Pursuant to Section 132 of the Administrative Procedures Act, if the Client fails to meet its obligations incorporated in the final decision of the Authority, the decision can be executed. Pursuant to Section 82(1) of the Administrative Procedures Act, the decision of the Authority becomes final with its communication. Pursuant to Section 133 of the Administrative Procedures Act, execution of the decision is ordered by the Authority adopting it, unless law or a government decree otherwise provides. Pursuant to Section 134 of the Administrative Procedures Act, the execution of the decision is carried out by the state tax authority, unless otherwise provided by law, government decree or, in the case of a municipal authority, the decree of the municipality. Pursuant to Section 61(7) of the Privacy Act, the Authority carries out the execution of the decision with respect to the performance of a specific act, specific behaviour, tolerance or ceasing as incorporated in the decision of the Authority.

Budapest, 8 February 2022.

Dr. Attila Péterfalvi
President
Honorary University Professor