Report

On the processing of personal data by artificial intelligence (AI) systems used by banks in Hungary

1. BACKGROUND

The European Union's Artificial Intelligence Act[1] (hereinafter: **AI Act**) was published on July 12, 2024. The AI Act officially entered into force on August 1, 2024. The provisions of the AI Act will be implemented gradually over the following years, with specific compliance deadlines for different categories of AI systems.

In Hungary, based on Act LXXV of 2025 (in force from 1 December 2025) and Government Decree 344/2025. (X.31.) on the implementation of the Act, the Hungarian Artificial Intelligence Council is entitled to issue guidelines and positions related to the implementation of the AI Act. Based on the above Member State legislation, the Minister of National Economy is responsible for the performance of the tasks of the market surveillance authority and the operation of the single point of contact pursuant to Article 70 of the AI Regulation, and the National Accreditation Authority performs the tasks of the notifying authority pursuant to Article 28 of the AI Regulation

On 7 July 2025, the Commission of the European Union issued guidelines on the definition of AI systems pursuant to Regulation 2024/1689 (**AI Act**).[2] Article 3(1) of[3] the AI Act also includes systems that generate predictions as outputs in the definition of AI systems. According to the guidance, '*AI systems using machine learning are capable of generating predictions that uncover complex patterns in data and make accurate predictions in highly dynamic and complex environments*', citing autonomous cars and AI systems measuring energy consumption as examples.[4] In contrast, simple forecasting systems *"(...) whose performance can be achieved via a basic statistical learning rule, while technically may be classified as relying on machine learning approaches fall outside the scope of the AI system definition, due to its performance*.[5]

---

[1] Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689

[2] Commission of the European Union, Commission Guidelines on the definition of artificial intelligence systems as defined in Regulation (EU) 2024/1689 (Artificial Intelligence Act) (29.7.2025) – hereinafter: **EC Guidance**

[3] 'AI system' means: machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments;

[4] EC Guidelines, paragraphs 54-55

[5] EC Guidelines, paragraph 49.

In its decision NAIH-85-3/2022, the **National Authority for Data Protection and Freedom** of Information (hereinafter: **Authority**) previously imposed a fine of HUF 250 000 000 on Budapest Bank Zrt. for unlawful data processing, which used artificial intelligence. In its decision, which is available in full in Hungarian[6] and English[7] on the Authority's website, the Authority concluded that, in the absence of adequate information, it is inherently difficult for data subjects to follow the use of AI and therefore providing information requires more - not less - effort on the part of the controller compared to processing based on earlier technology. The complexity of the subject does not exempt the data controller from its obligations[8] under the GDPR, the information to data subjects cannot be omitted just because the data controller also uses artificial intelligence. The existence of a right to object on paper does not comply with data protection rules either. If the data subject is unaware of the processing, then the data subject cannot object to it, especially if the data controller does not provide any practical means to do so before the processing takes place. If the legal basis of legitimate interest is used, the inadequate prior balancing of interests – which cannot be omitted and may not be exhausted in the presentation of the controller's own interests – affects the lawfulness of the processing. EDPB Opinion 28/2024[9] provides useful insights into how to carry out a balancing of interests when processing personal data for the training and use of AI.

The Authority sought an overview of which AI systems in the Hungarian banking sector are used for processing which type of personal data and how their legal compliance is achieved in 2025. Due to their current rapid spread and the volume of personal data they process, this type of processing is of particular importance from both a social and a data protection perspective. In that context, the Authority, inter alia, contacted the Hungarian National Bank and launched a number of separate ex officio investigations into the processing of data by banks operating in Hungary. In order to facilitate the development of good practices, the Authority publishes the results of its investigations in this report. The report is based on the replies to the questions sent to the banks that participated in the investigation. Because the purpose of the present report was to produce an overview, not to conduct a data protection authority procedure in

---

[6] https://www.naih.hu/határozatok-vegzesek?download=517:mesterséges-intelligencia-alkalmazásának-adatvédelmi-kérdései&start=100

[7] https://www.naih.hu/data-protection/decisions?download=522:ai-based-speech-signal-processing-technology-and-data-protection

[8] 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 (General Data Protection Regulation) (2016/679/EU) (hereinafter: **GDPR**): https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:02016R0679-20160504#C3-1

[9] https://www.edpb.europa.eu/system/files/2025-05/edpb_opinion_202428_ai-models_hu_0.pdf

order to establish the facts on the basis of evidence, the Authority did not examine the accuracy of the replies, and only reviewed them to filter out information protected by law.

2. EXECUTIVE SUMMARY

After examining the data processing operations covered by this report, the Authority highlights the following general good practices in the report. The report aims to fill a gap, its purpose is to raise awareness, not to fully cover the topic. There certainly are other good practices not covered by the report, as the report is based on a sample taken from only a part of the Hungarian banking sector, and aims to show to data controllers what good practices exist. This report is without prejudice to the legal obligations of data controllers and focuses on data protection compliance. Other Union or national legislation may impose different or additional obligations to data controllers.

One of the common applications of AI is to recognise images and read information from them. It is important to properly document or, if a third-party solution is used, obtain and record information about the source of training data for the AI model that converts images into data, which data was used, and how the accuracy of the AI model was measured. Since one of the results of identification is that the identified data subject gains access to the personal data - often sensitive banking personal data - of a given person, it is important for data protection purposes as well that the recognition is reliable. It is also necessary to select an appropriate retention period of the live image used for detection in order to comply with the GDPR principles of data minimisation and storage limitation, without compromising data security.

Recognition and processing of text and voice are currently popular uses of AI models, needed for example for the operation of virtual assistants. They are usually presented as an alternative to push-button control and, as long as they do not constitute automated decision-making under Article 22 of the GDPR (because they only serve to select a point in a menu instead of using buttons, or they only select the answer that most closely matches the question from a set of predefined responses or knowledge base, which can otherwise be found manually), they usually do not present a meaningful risk. The issues described in connection with image recognition should also apply here.

The knowledge of AI models is primarily not determined by the algorithm, but by the data used to train them. For this reason, the quality of the data used for training is important, as well as the fact whether or not the training data needs to be linked to a specific natural person. If it is only possible to train the AI model for a specific purpose with personal data, it is necessary to examine the conditions for legal basis or other use under Article 6(4) of the GDPR, and to adequately document the data source. In many cases, pseudonymisation (conversion into pseudonymous personal data) or anonymisation (non-reversible transformation into data that cannot be related to a specific natural person) can be used to mitigate privacy risks prior to training.

The use of 'Shadow AI' is a relatively new phenomenon. The generic term 'shadow AI' covers all cases where, in an organisation, users use individual AI systems in an unregulated, non-transparent, uncoordinated manner from the point of view of the organisation, either for work or for some personal use, using the organisation's IT infrastructure. Unlike the means used knowingly and with appropriate safeguards by data controllers, in such a case, the data controller's employees or subcontractors use AI to carry out or facilitate their own work without the data controller's knowledge. Because this way the data controller may lose control over a large amount of personal data and other data protected by law, the data controller must take appropriate steps to avoid this, utilising education as well as organisational and procedural safeguards. This is particularly the case for data controllers such as banks, which process a large number of sensitive data concerning many data subjects.

In their operations, the banks under review also use analytical models to analyse and predict creditworthiness and product affinity, the precise classification of which may raise questions. They often operate on a statistical basis, but may also have an AI-based part. From the point of view of data protection obligations, due to the technologically neutral regulation of the GDPR, it is irrelevant whether or not a given processing instrument is classified as AI, the basic conditions are the same for all processing instruments, and it is necessary to apply the appropriate safeguards to them based on all the circumstances of the processing.

The importance of anonymisation has been repeatedly raised in the topics discussed above. Practice in this regard is still under development. The EDPB is working on guidelines on pseudonymisation and anonymisation. Expectations in this regard also depend on the constantly evolving technical environment, as the protection of personal data must be ensured for the entire duration of the processing irrespective of which instrument is used for the processing. The rapid evolution of this environment also makes it difficult to define precise requirements.

3. AI USED TO PROCESS IMAGES

Hungarian banks are subject to customer identification obligations under Act LIII of 2017 on the prevention and combating of money laundering and terrorist financing (hereinafter: **Anti-money Laundering Act**) and the rules on the implementation of electronic customer due diligence using audited electronic communications device is laid down in Decree 29/2024. (VI. 24.)[10] of the Hungarian National Bank (hereinafter: **MNB Decree**). It is important to highlight the precise specification of the purposes of the processing and to separate processing based on a legal obligation from processing based on consent or legitimate interest. Thus, for example, the processing carried out in order to comply with the customer due diligence and reporting obligation laid down in the Anti-money Laundering Act is necessary for compliance with a legal obligation to which the data controller is subject, but if the data collected during the identification were to be used for the development of the algorithm, it would require the data subject's explicit consent. The unilateral extension of processing carried out in the context of a legal obligation or consent may in many cases infringe the principle of fair and transparent processing[11], as the data subject has no meaningful influence over the underlying processing. The Hungarian banking sector is increasingly using AI-component assets in its customer identification systems. When using such systems, they may use customers' own camera images as well as images and scans of customers' documents to identify customers. Banks can use a solution developed by a third party for these tasks, but there are also publicly available image databases to help them develop their own solution. However, the use of such tools must comply with the rules of the MNB Decree on indirect electronic customer due diligence.

3.1. Bank 1

In the process of opening an account online, the Bank 1 uses a non-real-time (indirect electronic) identification solution (identification based on a comparison between the self-portrait on the document and the facial image captured during the process). To do so, Bank 1 uses the service of a third party provider acting as data processor, who utilizes an AI system for the service. The successful identification process is followed by manual verification by a human both at the data processor and at Bank 1. If the identification has failed (the matching rate is below the threshold, including when the self-portrait is not perceived as a human face),

[10] 29/2024. (VI. 24.) Decree of the Hungarian National Bank on the detailed rules for the operation and operation of audited electronic communications equipment used by service providers supervised by the Hungarian National Bank, the minimum requirements of its internal regulations, the method of auditing and the implementation of electronic customer due diligence carried out by means of such equipment

[11] See EDPB Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models, paragraph 92

the identification process is concluded with this negative result and consequently the customer is not able to open the account in the online process. The possibility to open an account is also available through other channels (e.g. as a service provided in person in a bank branch or via an online video call). The retention period in the data processor's proceedings is in all circumstances 24 hours, after which the data processor permanently deletes the data used. After 24 hours, Bank 1 further processes the data specified in the Anti-money Laundering Act fulfilling its obligations under that law. The data processor's AI system consists of several components for which the data processor has different certificates of compliance.

3.2. Bank 2

Bank 2 uses an own customer authentication system with an AI component that utilizes a pre-trained open-source model. The system does not store any personal data, nor has the bank created a separate database. The solution runs on a dedicated bank server, where the central system sends the images and/or the video to the internal network and returns the result of the identification to the internal network. The solution used by Bank 2 has two components: on the one hand, it uses a pre-trained solution to verify and compare self-portraits with the image on the client's identity document, and on the other hand, an OCR system to scan the text of identity documents. The solution is suitable for online identification and conclusion of contracts, as well as for signing additional declarations. The system automatically performs face comparisons and liveness checks (whether there is a living person in front of the camera or a recording or a generated person), but the final check also involves a manual review by a bank employee.

3.3. Bank 3

In the case of Bank 3, an AI module was integrated into the system performing indirect electronic customer due diligence and was purchased as a product developed by a third party. The machine vision module cross-checks the images on clients' documents with the images taken during this process to confirm the identity of the client and to check whether the client is using the device in real time. The output of the process is used internally by the system: the data subject may either proceed to the next step in the screening process or be redirected to another type of screening or verification process. The AI module only processes images or data derived from images. These are stored in a temporary storage facility – a 'cache' – pending confirmation of identity. If the indirect customer identification system used by Bank 3 cannot successfully identify the customer with a sufficiently high level of certainty, the customer is automatically redirected to a manual process – direct electronic customer due diligence – i.e. in such cases a human review is always performed.

4. TEXT PROCESSING

In the banking sector, text processing tools using AI are typically virtual assistants, which can perform different tasks. Such virtual assistants automate tasks previously performed by human employees, i.e. providing general credit information to clients or potential clients, answering simple questions and making general credit calculations. This will make processes faster and more efficient, relieving the human workforce of routine tasks. A feature of such systems is that users depend on what data they provide, so they can provide any personal data, even without the need for it. It is therefore necessary for banks employing a virtual assistant to have procedures in place to filter unnecessary personal data and to store the necessary personal data (such as those used to identify customers) in a secure manner, while respecting the principles of purpose limitation and data minimisation.

4.1. Bank 1

In this context, Bank 1 uses a service integrated into a call centre and a written chat service. The former is controlled by the customer verbally, explains the subject of his call and, on that basis, the system connects him to the relevant case handler. In the chat service, the client receives a general answer based on the topical classification of the client's problem described in free text.

In the case of the call centre, Bank 1 uses the AI system only on the basis of natural language processing. Its use is optional for the customer and, in the absence of interaction, the call is transferred to a push-button system. The AI system of Bank 1 used for this purpose is self-developed, trained in a supervised manner by Bank 1 and does not learn new capabilities in the course of its operations. In order to build a separate training database, Bank 1 collected audio recordings from its customers, transcribed them manually and cleared the transcripts of personal data.

Within the chat service, Bank 1 shall use an AI component for the topic recognition function. If the client rejects twice the topic offered to him/her on the basis of his/her own problem description, he/she will be redirected to a manual topic selection interface. If there is no topic service for raising the issue, it is ultimately possible to refer the client to the case handler. The Bank 1 AI system used for this purpose is self-developed, trained in a supervised manner by Bank 1 and does not learn new capabilities in the course of its operations. For the training, Bank 1 has also set up a separate training database. To do so, it used the transcription of customer interactions within the service and manually removed personal data from them.

For both services, there may be service elements in which Bank 1 can only assist the customer through these channels if the customer authenticates himself. This identification method is implemented through a rule-based protocol where necessary, but according to its statement, Bank 1 does not use an AI component for customer identification in these cases.

4.2. Bank 2

A virtual assistant at Bank 2 is mainly used to provide general information about the services offered by the Bank, but may also perform more specialised tasks (such as credit calculations). In particular, the solution automates the tasks previously performed by the bank's employees, i.e. providing general credit information to customers and potential customers, answering simple questions and making general credit calculations. Users need to read and accept the Terms and Conditions and the Data Management Fact Sheet before they can start using the system. However, the software behind the system is provided by a third party provider based in the US, the relevant details of the messages provided by the users and of the publicly available documents of Bank 2 are transferred for processing by the third party model. The bank server communicates with the third party service provider server as an intermediary, so that the IP address or other identifier of the user customer is not known to the third party, only the IP address of the bank server is visible. However, in addition, the user may enter personal data in the text of the query and, in this case, it will be transferred to the third party to process the question. This operation is brought to the attention of users in the Data Management Factsheet.

4.3. Bank 3

Bank's 3 digital assistants are an integral part of the mobile bank application and are used for digital communication with customers. This service operates in two different ways: in the first case, it interacts with users without prior request, typically sending push messages with information, and in the second case, users can engage in conversations when asking questions. In some cases, the virtual assistant replies that he or she directs the customer to the mobile banking functionality he or she wishes to use, but these functionalities can be accessed without the assistant's intermediation, it only directs the user to the corresponding menu option. If the solution fails, the customer will be redirected to the human channel, e.g. a phone handler. The solution does not use an external (third party) component and uses the bank's internal systems to retrieve the necessary data. The solution uses an AI language model to interpret the client's instructions in natural language (a transcription into voice, similar to the one currently used by the Authority[12]).

[12] https://naih.hu/adatkezelési-tájékoztatók
'Privacy notice for the Authority's processing operations in the context of the conduct of public authority procedures for the enforcement of requirements relating to the protection of personal data and the disclosure of data of public interest or made public on grounds of public interest', point 6.3.

5. DATA USED TO TRAIN

The training of AI does not always require the use of data related to a natural person. Due to the principle of data minimisation, where possible, the training of the AI model should in principle be done with anonymous data. Where data collected for other purposes are used, including by means of anonymisation, it can take place on the appropriate legal basis (or by justifying the conditions under Article 6(4) of the GDPR) and by informing the data subjects, as the anonymisation of personal data is also a processing operation.

5.1. Bank 1

Bank 1 did not use the personal data of its customers to train the Client Identifier AI system and acquired the system from a third party who had already trained it.

5.2. Bank 2

Bank 2 has created an additional database of documents produced, verified and disclosed by the bank, and the AI solution provided by a third party searches for the data necessary to answer the question put to the assistant from a database that stores information not related to that person and does not use any personal data to generate the answers. The virtual assistant uses the solution of a third party and does not train the model, but only develops the additional 'knowledge pool' database (e.g. content of standard contractual clauses, factsheets, etc.). The model provided by the third party does not have access to the bank databases or to the internal systems of Bank 2. The dataset developed by Bank 2 was designed to cover the most common issues related to the products offered by Bank 2. The system selects the relevant whole paragraph or sentence from the ready-made answers, and uses them to generate answers optimized to the question.

5.3. Bank 3

In the case of Bank 3, the new data used to train the text AI model come from the experience gained in analysing anonymised log entries and from developers. The data used in the training are simple Hungarian words, sentences that do not contain any personal data or data covered by banking secrecy. Labelling is done manually in several rounds to determine first their suitability, then their belonging to the appropriate group (intent), and then to identify the priority entities in the sentence.

In case of the training of the model for the machine vision solution used by Bank 3, no access was given to the personal data it processes, the solution was acquired as a product from a third party.

6. SHADOW AI USE

Shadow AI obviously poses a data security risk, as in such cases the organisation does not have control over such data processing running on its own IT infrastructure (for example, whether the user uses an AI system that has access to the data processed on the internal network during its operation; whether the user uses the AI system to facilitate his/her work; whether the user uses personal data processed by the organisation in interactions with[13] the AI system, in particular prompts, etc.)

6.1. Bank 1

The current modus operandi of Bank 1 prohibits the use of AI tools that do not run on the Bank 1 infrastructure. In practice, the restriction is ensured by technical prohibitions. Only devices that are protected by a Single Sign in System (SSO) and data separation are accessible to staff. Some AI systems are allowed for dedicated users. These AI systems are available, subject to security settings and limitations, to authorised users, who have also received a user manual on ethical use in accordance with internal policies.

6.2. Bank 2

Bank 2 prohibits the use of 'shadow AI' within its organisation and in order for the bank to enforce the prohibition, a content filtering service has been introduced, so it is not possible to visit pages in the prohibited category.

6.3. Bank 3

Bank 3 also prohibits the use of 'shadow AI', but in addition, the bank's parent company has a unique global contract with a service provider, whereby Bank 3 employees can use the service provider's AI assistant while excluding the use of usage data for model training. A wide range of customisable rules and alerts can be set for each user's activity, strengthening the control environment.

7. CREDITWORTHINESS AND PRODUCT AFFINITY CALCULATION

The reviewed banks use several types of technical solutions in their operations. Some of these cannot be clearly identified as AI. Decision-supporting analytical models can create a customer profile based on several aspects (such as credit risk or fraud prevention risk assessment). The prediction issued by these tools can be related to a variety of products or services, such as credit, investment or card service. Because it is difficult to distinguish some of these use cases,

---

[13] Prompt is an input instruction, question or other user interaction on the basis of which AI generates an answer or content.

those who use such tools must pay special attention to the way the decision-making models work. The EC Guidance mentioned in section 1 above may help with AI classification. However, from a data protection point of view, due to the technology neutrality of the GDPR, the theoretical data protection requirements are independent from the technical classification of the device used for data processing, as they prescribe results instead of governing devices.

7.1. Bank 1

In the context of its cookie processing activity, Bank 1 uses, based on consent as a legal basis, targeting and advertising cookies that enable targeted marketing tailored to the interest of the visitor to the website. As communicated by Bank 1, promotions are presented using machine learning models and/or rule-based models. Subject to the consent of the visitor to the website, Bank 1 may use the data collected through the use of cookies in combination with the customer's personal data available at Bank 1, allowing for a more individualised response.

In its sales promotion activities, Bank 1 performs calculations to recommend a suitable product to the customer or to assess whether that product is available to that customer. The product affinity score supports the recommendation of the product that best suits the client, and the credit score helps assess the client's creditworthiness. Bank 1 has made such calculations through human resources in the past, but is also currently using AI systems.

The product affinity score represents the value of the probability of selling banking products for that customer. The AI system scores each banking product based on how likely the customer is to use that product in a given month. The AI system captures this variable from the combination variations of different data groups. The values thus generated are only accessible to the administrator and no further data are generated. The score supports the work of the case handler, but it does not bind the case handler or the data subject to anything. The score data generated shall not be used by Bank 1 for other purposes and customers shall not be classified on this basis. The AI system is entirely internally developed (development, operation, training takes place within Bank 1).

A credit score is a value produced on a statistical basis as an element of the credit scoring process. It is produced to measure the customer's creditworthiness. Classification on this basis is an indication of the probability of the customer applying for a loan becoming insolvent within 1 year. The resulting rating value is an element of the evaluation system, but not the decision point. Bank 1 shall use a proprietary model for this purpose. It carries out both development and operation independently. The model is not self-learning and is subject to monthly monitoring with human oversight. From the training database, Bank 1 removed the personal data and linked the related data elements through a special identifier. The model was tested first with the test data thus generated, then with real-world data, but still (instead of production) in an integrated test environment. The test does not involve the allocation of rights which could result in the staff member having access to data to which they do not otherwise have access. There shall be no modification or deletion of the data in the form in which it is stored in production.

Fraud screening, a strong level of data security, customer identification and broader credibility are central issues in Bank's 1 activities. In this respect, a number of legal provisions must also be complied with. The purpose of the AI system used in this context is to prevent, detect, investigate and monitor fraud involving payment cards, bank accounts and the misappropriation of electronic identification data.

7.2. Bank 2

Bank 2 does not apply AI tools to profiling related to the sale of products or to marketing and profiling related to commercial activity at the relevant time.

7.3. Bank 3

Bank 3 uses models for marketing purposes whose function is to provide marketing experts with information on which products, channels and communications may be relevant to customers.

The purpose of the credit risk models used by Bank 3 is to support responsible lending practices required by law. The output of these models is a number that denotes credit risk and, like marketing models, is used to support expert judgement. The purpose of credit risk models is to support responsible lending practices that are required by law.

8. THE CONCEPT AND IMPORTANCE OF ANONYMISATION IN AI-RELATED DATA PROCESSING

The questions of processing of personal data provided during chats with the personal assistant and the removal of personal data before the conversations were logged have arisen for multiple banks during the review. In some cases the technical specifications include the expression of depersonalisation in this context, along with anonymisation. In this context, it is necessary to clarify that anonymisation[14] and pseudonymisation[15] exist from a data protection point of view, depersonalisation is not a legally defined concept.

---

[14] According to recital 26 of the GDPR, anonymised data means 'information, *which does not relate to an identified or identifiable natural person and (...) which has been anonymised in such a way that the data subject is not or no longer identifiable*'.

[15] According to Article 4(5) of the GDPR*, the term 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of*

8.1. Bank 1

For the topic recognition module, Bank 1 generated the training data from the transcription of customer interactions within the service, with their manual anonymisation. The credit scoring module model is not self-learning and learns on a monthly basis with human oversight. Bank 1 removed personal data from the training database and does not use personal data to train the model. Testing does not involve the allocation of access rights which could result in a bank employee having access to data to which they would not otherwise have access in their day-to-day work.

8.2. Bank 2

Conversations with a virtual assistant employed by Bank 2 shall be stored until the conversation is closed by the user, but no longer than 30 minutes after user inactivity. They are then anonymised and the anonymised text is stored on the bank's own servers for the time necessary to develop the system. Anonymisation is performed by an NLP[16] -based algorithm that searches for personal data in the conversation based on predefined parameters and deletes them before storage.

8.3. Bank 3

Bank 3 uses the conversations of users with the digital assistant to improve it, but they are anonymised before being used for this purpose. First, a chat log is produced containing the first free text sentence of the conversation with the customer and an assessment of whether the passive digital channel gave the correct answer or, if not, which answer should have been invited to the sentence. There is also a 'chat ID' assigned to the conversation (pseudonymised processing), but the Hungarian sentences to be used for training are then selected, while deleting all other data. A further check of the logs thus retained precedes their use for training.

additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

[16] NLP: The 'Natural Language Processing' algorithm is a type of AI-enabled algorithm that processes and analyses natural languages, such as Hungarian.