Is there no new thing under the Sun, or considering the practice of the EU authorities, does the GDPR provide answers to the data protection questions the use of artificial intelligence raises?

Table of contents

1. Introduction, description of the issue to be addressed

The fact that technology is developing at an extremely accelerated pace is hardly questionable, the spread of artificial intelligence (AI) and its various types is unstoppable, and AI-based software is increasingly becoming part of our everyday lives in many areas.

In many cases, the use of AI involves the processing of personal data, which means that data protection issues cannot be avoided when designing, writing and using software based on the use of AI.

The aim of this thesis is to examine what the main data protection issues raised by the design and use of artificial intelligence systems involving the processing of personal data in the light of the European Union's General Data Protection Regulation (GDPR) are, whether the practice of the authorities in the field of artificial intelligence shows that the GDPR contains an adequate level of regulation, which does not require new rules from a data protection perspective, but only the proper application of existing rules, or whether there is, or could be, a need for legislative action in this area.

Given that there is currently no legal definition of AI, this thesis necessarily takes as its starting point the definition of AI as proposed by the European Commission in its proposal for a Regulation on AI[1] (the Proposal), and as proposed by the European Council and then the European Parliament in their proposal for a Regulation on AI. According to the Proposal, *"'artificial intelligence system' (AI system) means software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with"*[2]. The definition proposed by the European Council defines an AI system as follows: *"'artificial intelligence system' (AI system) means a system that is designed to operate with elements of autonomy and that, based on machine and/or human-provided data and inputs, infers how to achieve a given set of objectives using machine learning and/or logic- and knowledge based approaches, and produces system-generated outputs such as content (generative AI systems), predictions, recommendations or*

[1] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules for artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (Brussels, 21.4.2021 COM (2021) 206 final 2021/0106 (COD)).

[2] Article 3(1) of the proposed Regulation.

decisions, influencing the environments with which the AI system interacts"[3]. According to the definition proposed by the European Parliament, *"artificial intelligence system' (AI system) means a machine-based system that is designed to operate with varying levels of autonomy and that can, for explicit or implicit objectives, generate outputs such as predictions, recommendations, or decisions, that influence physical or virtual environments"*[4]. This thesis makes no attempt to analyse the three techniques and approaches listed in Annex I of the regulation as per the Proposal[5], or the AI definitions proposed above, but instead takes as a point of reference the very broad definition of AI as proposed, according to which essentially all software is considered to be AI, which performs some kind of an operation on the basis of input data (with or without the help of machine learning), which has an "output result", *i.e.* the program is able to draw some conclusion, or possibly make a decision, on the basis of the data and information provided, which then it makes available to the user of the AI. It is worth noting that, from a data protection point of view, in my opinion, the amendment proposal containing the Parliament's negotiating position does not contain anything new which would not follow from the GDPR[6].

[3] See the Council's "general approach" of 25 November 2022. Council of the European Union, *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts - General approach* (https://data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/en/pdf) (accessed on 27 August 2023), p. 71.

[4] See the document on the European Parliament's negotiating position adopted on 14 June 2023, which contains hundreds of proposals to amend the text of the proposed AI Regulation. European Parliament, *Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM (2021) 0206 - C9-0146/2021 - 2021/0106(COD)) (1)* (https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html) (accessed on 27 August 2023).

[5] These are as follows: (i) machine learning approaches, (ii) logical and knowledge-based approaches, and (iii) statistical approaches, Bayesian estimation, search and optimization methods.

[6] The Parliament's proposal lists six principles that apply to all AI systems: (i) human oversight of the AI system, (ii) technical resilience and security, (iii) privacy and adequacy of data processing, (iv) transparency, (v) diversity, non-discrimination and fairness, (vi) social and environmental well-being, and would prescribe certain obligations depending on the type of AI (*e.g.* for certain AI systems considered to be high-risk, a fundamental rights impact assessment and consultation with public authorities would be required, or, in the case of generative AI systems, public disclosure of the use of copyrighted data used to teach the system would be expected).

This paper approaches the questions raised (*i.e.* what kind of caution is advised from a data protection perspective when using artificial intelligence, what are the relevant issues that arise in connection with the use of this type of modern technology) from the perspective of the provisions of the GDPR, including the principle of data protection by design and by default as laid down in Article 25 of the GDPR and the obligations arising therefrom, and, in particular, Article 22 of the GDPR, the "prohibition" stipulated in Article 22[7] and the requirements for automated decision-making.

2. Privacy by design and by default

Where personal data is processed, whether or not using artificial intelligence, it is necessary to comply with the provisions of the GDPR, and the provisions of the GDPR will necessarily apply to the use of AI.

2.1 Article 25 of the GDPR

The principle of data protection by design in Article 25 (1) and the principle of data protection by default in Article 25 (2) of the GDPR impose an obligation on all controllers, regardless of the type of controller and the complexity of processing.

According to the principle of data protection by design, the data controller is obliged to establish and implement appropriate technical and organisational measures, both at the time of determining the method of data processing and during the processing, to ensure compliance with the principles and requirements of the GDPR and to provide effective and guaranteed protection of the rights of data subjects. The controller must do so taking into account the state of the art, the cost of implementation, the nature, scope, context and purposes of the processing and the varying likelihood and severity of the risk to the rights and freedoms of natural persons which the envisaged processing may pose.

The principle of data protection by default requires each controller to design and implement appropriate technical and organisational measures to ensure that personal data are processed only for the specific purposes for which they are intended by the controller. This necessity includes, *inter alia*, the number of personal data collected and the duration of processing.

[7] In essence, as a general rule, the provision set out in Article 22 (1) of the GDPR prohibits decisions based solely on automated processing which would produce legal effects concerning the data subject or which would similarly significantly affect him/her.

If the essence of Article 25 (data protection by design and by default, "DPbDD") were to be defined in one sentence, one could say that the controller is obliged to consider before processing how the envisaged processing will comply with the principles of the GDPR and other requirements, *e.g.* on data security, and how it can maintain compliance in an effective manner (by modifying or adapting certain features of the processing, where appropriate) on an ongoing basis throughout the processing. In the words of the European Data Protection Board: "*Controllers shall implement DPbDD before processing, and also continually at the time of processing, by regularly reviewing the effectiveness of the chosen measures and safeguards."*[8]

By explicitly referring to the data protection principles, Article 25 reiterates the principles set out in Article 5 of the GDPR, out of which, in the case of data processing by way of using AI, the principles of fairness, transparency, purpose limitation, data minimisation and accuracy are paramount. (Of course, other principles must also be met, such as the principles of lawfulness, storage limitation, integrity and confidentiality, and accountability.) The GDPR does not prescribe the specific measures to be taken by the controller, so controllers must themselves plan and design the measures for the processing they intend to carry out in a timely manner to ensure ongoing compliance with the legal requirements.

When judging compliance, "ongoing efficiency" is key. The obligation in Article 25, like many other obligations in the GDPR, is not a static obligation, but a dynamic, ongoing requirement, and in order to comply with it, the GDPR provides guidance on the different aspects the controller needs to take into account[9].

As regards the appropriate technical and organisational measures, Article 25 essentially refers to Articles 24 and 32. The former imposes an obligation on data controllers, essentially formulating the principle of data protection by design in a slightly different way, while the latter article imposes an obligation on both the controller and the processor to ensure adequate data security.

The risk-based approach is emphasised, given that a certain risk and its existence or non-existence are not static, and therefore the measures to be taken cannot be taken once and for all, as they are intended to address changing risks. The data controller (and also the data

[8] European Data Protection Board Guidelines 4/2019 on data protection by design and by default under Article 25, version 2.0 (date of adoption: 20 October 2020), p. 4.

[9] The state of the art, the cost of implementation, the nature, scope, context and purposes of the processing, and the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing.

processor under Article 32) must assess these risks, their likelihood and severity in advance and, on the basis of the analysis, take appropriate measures to ensure compliance with data protection law. Although, data protection impact assessment (DPIA) is not specifically addressed in this paper, it is worth noting that, in the case of processing through the use of AI, particular attention should be paid if a DPIA needs to be prepared prior to the start of the processing, which in many cases could be the case due to the technological novelty artificial intelligence means[10], or, even if an impact assessment is not necessary in a particular case, it is useful to document how the controller has come to this conclusion, and it may be worth testing the algorithm by feeding it with "test data" and then observing how modification of the data changes the functioning of the algorithm.

Adequate prior identification of the risks posed by the envisaged processing is essential, without which the controller (or processor) will not be able to take appropriate measures to address the risks, which will necessarily mean non-compliance.

Compliance with Article 25 of the GDPR is also important because when it comes to imposing a fine under the GDPR, authorities must take into account the extent of the controller's or processor's liability, the technical and organisational measures they have taken pursuant to Articles 25 and 32[11].

2.2 AI from the perspective of Article 25

The above is applicable to data processing when using AI, but is particularly relevant when an organisation designs, tests and uses AI software, given that AI technology is particularly likely to exacerbate existing risks, create new risks or make existing risks more difficult to manage[12].

The Guidelines of the European Data Protection Board emphasise that *"[e]arly consideration of DPbDD is crucial for a successful implementation of the principles and protection of the rights of the data subjects. Moreover, from a cost-benefit perspective, it is also in controllers'*

[10] Depending on the characteristics of the processing, the need to carry out an impact assessment can also be inferred from Article 25. It is also outside the scope of this paper, but it is worth briefly mentioning that a so-called fundamental rights impact assessment may also be required before the start of certain processing using artificial intelligence, on the basis of the forthcoming Artificial Intelligence Regulation.

[11] Article 83 (2) (d) of the GDPR.

[12] Information Commissioner's Office, *Guidance of AI and data protection* (https://ico.org.uk/media/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection-2-0.pdf (accessed on 3 August 2023), p. 8).

interest to take DPbDD into account sooner rather than later, as it could be challenging and costly to make later changes to plans that have already been made and processing operations that have already been designed"[13].

There are several main phases in the application of AI software, the first of which is design, followed by development, test use, followed by live use, real-life application (including continuous monitoring and supervision of the system's operation), and finally, the end of the software's use.

3. Specific GDPR provisions and the AI

The GDPR does not contain the term artificial intelligence, but its rules apply to any activity that involves the processing of personal data.

While the difficulties in aligning AI-based technology with the GDPR include compliance with the principles of transparency[14], purpose limitation, data minimisation and accuracy, giving adequate information and ensuring data subjects' rights, it is certainly an exaggeration to say that the GDPR would make the use of AI impossible to implement, one could rather say that it is more time-consuming and costly to operate an AI model in a compliant way[15].

It is often said that certain provisions of the GDPR are not concrete enough and do not provide sufficient guidance for entities considering data processing. Indeed, the GDPR contains "neutral" provisions (*e.g.* requiring the taking of "appropriate technical and organisational measures"), the application of which requires balancing between competing interests and, in the case of AI, the novelty and complexity of the technology and the extent of its impact on individuals make the issues even more pronounced[16]. However, there is no expectation of "zero

[13] European Data Protection Board Guidelines 4/2019 on data protection by design and by default under Article 25, version 2.0 (Date of adoption: 20 October 2020), point 36, p. 11.

[14] Alan Turing said as early as the 1950s that a machine with the ability to learn will achieve its goals in ways that its creators and teachers could not foresee, in some cases without knowing the details of the machine's inner workings. This "black-box" phenomenon is specific to certain AI models.

[15] In my view, one can agree with the approach in the proposed AI Regulation (shared by the European Council and the European Parliament), meaning that some AI-based processing should be prohibited in principle, given its highly invasive nature, while other AI-based processing as high-risk processing should be subject to specific additional conditions, but these are not the subject of this paper.

[16] The impact of the General Data Protection Regulation (GDPR) on artificial intelligence, Study Panel for the Future of Science and Technology, EPRS | European Parliamentary Research Service, Scientific Foresight Unit (STOA), PE 641.530 - June 2020, Executive summary, p. III.

tolerance" of risks, in which case no data could be managed, the focus is on striking the right balance[17]. In the following, I will mention the main points of conflicts in relation to the principles, legal bases and data subjects' rights that are particularly relevant in the context of an AI-based data processing.

3.1 The data protection principles and the AI

3.1.1 Transparency and fairness

These principles mean, on the one hand, that concise and comprehensible information must be provided to data subjects[18], and on the other hand, that, for example, when profiling is carried out, the controller needs to apply technical and organisational measures (including mathematical and statistical procedures) to ensure that the factors that cause inaccuracies in the data are corrected and errors are minimised. Similarly, the controller must take into account factors that pose a risk to the rights of the data subject and ensure that the processing is non-discriminatory[19]. This is particularly relevant in the case of automated decision-making.

In the light of these principles, it should also be considered whether "re-identification" is possible, *i.e.* if, due to technological developments or even the circumstances of data processing, (*e.g.* machine learning) a person may subsequently become identifiable despite the fact that, for example, pseudonymisation was originally used.

Ensuring transparency can mean quite a challenge, especially in the case of machine learning[20], when the author of the software does not know (even despite his/her best intentions) exactly why the machine is reaching a particular conclusion. In such a case, the applicability of the technology is questionable, since if the author does not know how the model works, nobody will, including the data subject.

If the data are collected directly from the data subjects, the information must be provided to the data subjects at the time of collection, before the model is taught or, respectively, before the model is applied, whereas if the data are not collected from the data subject, the information

[17] Information Commissioner's Office, op. cit., p. 13.

[18] GDPR (58) Recital.

[19] GDPR (71) Recital.

[20] The Information Commissioner's Office, the UK's data protection watchdog also stresses that it can be a significant challenge to provide a clear explanation of how AI works. See Information Commissioner's Office, op. cit., p. 7.

must be provided within a reasonable time, but not later than one month, or earlier if and when the data subject is contacted or when the data are transferred to another person.

The question may arise as to the applicability of Article 14 (5) b) of the GDPR, which provides that information need not be provided where *"the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for… scientific or… research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89 (1)…"*. However, the GDPR also requires in such a case that the controller takes appropriate measures to protect the rights of the data subject.

3.1.2 Purpose limitation

One feature of AI models is that they allow data collected for one purpose to be used for another. For example, the use of a "Like" button to express an opinion can be used to infer psychological characteristics, political opinions, consumer habits.

The GDPR provides that data may not be processed in a way incompatible with the original purposes, adding that further processing for purposes such as scientific research or statistical purposes is not incompatible with the original purpose (if it complies with Article 89 (1))[21]. The legislation also provides guidance on what criteria may help to determine whether the new purpose is compatible with the original purpose when processing is not based on the data subject's consent or on EU or Member State law[22]. The question is what can be considered compatible with the original purpose in the context of the use of AI.

For example, in the case where an AI model is trained to predict certain health risks to participating individuals based on the health data provided, it is highly unlikely that the individual concerned could not legitimately object if the database were then also used to offer insurance premiums to the individuals based on inferences drawn from the provided health data. The former use could clearly be beneficial for the data subject, as it could make it possible to detect a potential disease in time, but the latter could be extremely disadvantageous and discriminatory for the data subject.

The issue of data processing other than for the original purpose often arises, for example, in relation to large data sets, where newer and newer correlations may be revealed through data analysis. The question is where the line is/can be drawn between data processing that is

[21] Article 5 (1) (b) of the GDPR.

[22] Article 6 (4) of the GDPR.

compatible and incompatible with the original purpose. This will of course require a case-by-case analysis, but the GDPR states that for processing compatible with the original purpose of the processing, *"no legal basis separate from that which allowed the collection of the personal data is required"*[23].

For example, if pseudonymised or encrypted data used to teach a model algorithm is used for statistical purposes (*i.e.* for a purpose other than the original purpose), it may be compatible with the original purpose. However, if the same data was used for profiling an individual, this may go beyond the limits of compatibility[24].

3.1.3 Data minimisation

There seems to be an obvious contradiction between the principle of data minimisation and especially the processing of big data by artificial intelligence, since the latter is basically "interested" in getting access to as much data as possible in order to be able to draw conclusions and patterns (and learn from them).

It is important to note here that the words "as much data as possible" should not be taken literally, as the AI model is not interested in collecting data irrelevant (and/or inaccurate) for the purposes of the operation of the model, as this would undermine the reliability and thus the usability of the model. It is essential that the data are relevant and representative for the given purpose, otherwise it is certain that the model will not work properly and serious biases and discriminatory operation can be expected.

3.1.4 Accuracy

AI-based algorithms can only be as good as the data used to teach them are, thus, good quality data is essential for quality algorithms[25]. It is important to ensure that the input data is accurate

[23] Recital (50) of the GDPR.

[24] A particular issue is the processing of special category data, especially when the AI draws conclusions from non-special category data, which already qualify as special category data, such as when the algorithm draws conclusions from shopping habits and the analysis of "liked" content and comes to conclusions concerning psychological/health characteristics, sexual orientation, political opinions, which may be used to attempt to unconsciously influence the given person (for example, to sell certain products to them) or discriminate against them.

[25] The *"garbage-in, garbage-out"* principle. European Union Agency for Fundamental Rights, *Data quality and artificial intelligence - mitigating bias and error to protect fundamental rights*, 2019

from the moment the AI model is taught, especially when the data is used to make inferences or decisions about the data subject. Inaccurate data may in itself cause harm to the data subject, for example, if it is processed in a way that does not match its characteristics. At the same time, the accuracy of the output data should be ensured in such a way that it is based on accurate input data and the model performs the calculations correctly based on a "well-weighted" algorithm. It should be noted, however, that compliance with the principle of accuracy does not imply that the model must be statistically 100% accurate[26]. Some models are used to predict certain probabilities (*e.g.* susceptibility to illness, likelihood of late payment), so it is not *a priori* the case that the output of the model (the prediction) is definitely accurate (this fact must also be stated in the privacy policy).

If an AI system is used to draw conclusions about individuals, it must be ensured that the system is statistically sufficiently accurate for the given purpose. This does not mean that all inferences have to be correct, but the possibility that inferences may be wrong and the impact this may have on the decision made on the basis of the inference must be taken into account. Failure to do so may mean a breach of the principles of fairness, accuracy and data minimisation (the latter because incorrect personal data may not be adequate and relevant in relation to the purpose).

It is essential to address false assessments (false positives, false negatives). For example, in the case of a CV pre-screening model, if the system recommends inviting for an interview someone who does not match the characteristics of the candidate looked for, energy and time is wasted, whereas if the system does not recommend inviting for an interview someone who would be an ideal candidate, an opportunity may be lost for both the employer and the candidate.[27]

3.1.5 Storage limitation

In relation to this principle, it is worth noting that the storage of personal data for longer than necessary is allowed where the processing of personal data is carried out for purposes such as scientific research or statistical purposes (in accordance with Article 89 (1) and provided that appropriate security measures are taken to safeguard the rights of the data subjects).

(https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-data-quality-and-ai_en.pdf (accessed 31 July 2023), p. 1).

[26] Information Commissioner's Office, op. cit., 39 p.

[27] Information Commissioner's Office, op. cit., p. 41.

3.2 The legal bases and the AI

In order to specify the legal basis, it is important to name the purpose of the processing. In the case of a machine learning model, a distinction needs to be made between the development-design-learning phase and the application phase of the model[28]. The learning of the model itself does not necessarily have a direct consequence for the data subject, but direct consequences should be expected when the model is applied to the data subject.

Out of the legal bases for the use of AI, the most relevant are the consent of the data subject and the legitimate interest of the controller[29]. The difficulty with the former is that it is not easy to fulfil all of its conditions, and it is difficult to obtain consent if there are a lot of data subjects, in addition, the data subject can withdraw his/her consent unconditionally at any time, a possibility that the controller should also take into account in advance.

Also, in terms of legitimate interest, a distinction should be made between when data is collected to teach an algorithm and when an algorithm is already in use and the data is an "input signal" that the model processes based on the algorithm (and, respectively, based on what it has learned) and provides a response. In the former case, the applicability of legitimate interest seems more obvious, provided, *inter alia*, that there is a legitimate purpose for the processing and that the necessary security measures are taken (*e.g.* pseudonymisation, encryption). In the latter case, it needs to be carefully examined if the legitimate interest of the controller can be used as legal basis or if rather the data subject's consent can be the legal basis or not even consent can be relied upon.

Although, legitimate interest is the most flexible legal basis for data processing, it is not always the most appropriate. For example, in cases where the use of personal data is not expected by the data subject or could cause unnecessary harm to the data subject, it may not be the appropriate legal basis. The use of legitimate interest also implies that the controller assumes

[28] For example, one develops a facial recognition software that can later be used for various purposes (*e.g.* authentication, tagging friends online).

[29] Article 6 (1) (b) of the GDPR may be more of a legal basis when applying the model to the data subject (less so when teaching the model), but only if the service cannot be provided with less intrusive processing and the processing is objectively necessary, for example, for the performance of a contract with the data subject. The use of legal bases under Article 6 (1) (c), (d) and (e) of the GDPR is not *per se* excluded, but is typically unlikely. The legal bases under clause (d) can be essentially excluded for the teaching of an AI model, while at the same time the applicability of clause (d) could be considered for the application of the AI model to the data subject, possibly in the case of a given medical use.

an additional responsibility for the protection of the rights of data subjects and has the obligation to justify the necessity and proportionality of the processing[30].

3.3 The rights of the data subjects and the AI

The GDPR declares in Article 1 that it *"protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data"*.

The focus of the GDPR is on the data subject, his/her protection, and each provision is designed to protect the data subject, thus, the rights of the data subject are closely linked to, among others, the principles, including the provisions of Article 25.

I will briefly raise below the issue of AI and certain rights of the data subject, with a focus on the "right" in Article 22, which is also the subject of the case law discussed in Sections 4.1 and 4.2 below.

3.3.1 Right of access

One of the questions that arises in relation to the right of access is to what extent the rights of others may constitute an obstacle to the exercise of this right, for example, whether the right to information may be denied on the grounds of the copyright of the developer of the AI model. According to the GDPR, the right of access *"should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software"*, but it is also clear that not all information can be withheld from the data subject on this basis[31].

3.3.2 Right to rectification

Ensuring this right with respect to the data used to teach an AI model typically does not affect the operation of the model in any substantive way, but it is questionable whether it is technically feasible to ensure this right. With regard to the personal data generated by the application of the model to the data subject, it is less likely to be technically unfeasible, adding that the right to rectification should be ensured both in the learning process and in the application of the AI.

[30] This is demonstrated by the so-called legitimate interest assessment (also known as balancing test) and, where appropriate, the data protection impact assessment. If such a document is prepared during the development and training phase of the AI, it will need to be reviewed as and when the data processing purposes become more specific, are supplemented, or, respectively, as the case may be, another legal basis may be required.

[31] Recital (63) of the GDPR.

3.3.3 Right to erasure

Regarding the right to erasure, an interesting question is whether, if the collected data used for training is to be deleted from an AI model, only this data should be deleted, or also the data inferred by the algorithm from the data used for training. It is also a question that if only the collected data is to be deleted, what effect the deletion can/will have on the model's performance.

Where appropriate, the conditions of Article 17 (3) (b) may have to be examined, according to which the data need not be erased if, for example, they are processed for scientific research or statistical purposes (in accordance with Article 89 (1)), where the right to erasure would be likely to render the processing impossible or seriously jeopardise it. Considering that the deletion of a single piece of data is unlikely to have a major impact on the functioning of a larger database, any successful reference to this provision seems questionable.

3.3.4 Right to data portability

The right to data portability covers the data collected from the data subject (used for teaching the AI) if processing is based on the data subject's consent or on Article 6 (1) (b) (in the case of use of AI, processing necessarily takes place by automated means), but not the output data inferred from the data received.

3.3.5 Right to object

As regards the right to object, it is worth mentioning that the data subject has this right, *inter alia*, in cases of processing based on the controller’s or a third party’s legitimate interest and for direct marketing purposes, or when processing is carried out for purposes such as private scientific research or statistical purposes. The controller must also ensure that this right is guaranteed, including in cases of profiling based on legitimate interest or in connection with direct marketing.

3.4 Automated decision-making and the AI

With regard to AI, Article 22 of the GDPR is of high importance, as some AI models are used exclusively for automated decision-making. In addition to the fact that such processing is in principle prohibited[32], in the case of such automated decision-making, the controller must

[32] Article 22 (1) of the GDPR.

provide information on the logic used[33], the significance of the processing and the envisaged consequences for the data subject[34]. At the same time, where automated decision-making is based on the explicit consent of the data subject or is necessary for the conclusion or performance of a contract between the controller and the data subject, the controller must take appropriate safeguards to protect the rights of the data subject and ensure at least that the data subject may request human intervention, express his/her view and contest the decision[35]. It should be noted that Recital (71) of the GDPR also mentions two further elements among the appropriate safeguards, namely, the provision of specific information to the data subject and the "right" to obtain explanation of the decision taken on the basis of the assessment. The requirement to provide specific information is not necessarily understandable, given that this obligation is provided for in Articles 13 and 14, but it is questionable whether the provision of an explanation is always mandatory (the expression "at least" in Article 22 (3) may even imply this, but it cannot be excluded that it is only a quasi-recommendation and that it is appropriate to provide an explanation where justified by the circumstances). In my view, it is appropriate to provide an explanation, even if Article 22 does not contain such a requirement, in order to ensure greater transparency.

In the case of profiling and automated decision-making, ensuring non-discrimination is of particular importance and it may therefore be important that AI-based automated decision-making has a meaningful human review built into the system and that the model is continuously monitored. For example, if a bank is using software to rate a person's creditworthiness and it becomes clear during its operation that, for some reason, the algorithm consistently assigns a lower score to female loan applicants, then the software is clearly discriminating (*e.g.* because much less data is entered for women and the algorithm is not weighting women appropriately, or because it is biased towards women in a way that they are more likely to default)[36]. In such cases, the quality and ratio of the input data needs to be improved, or the data, the training process and/or the model should be modified to ensure that the algorithm is not biased.

Measures must also be taken (through internal rules and training) to ensure that, when using AI to support human decision-making, the person in a decision-making position who is

[33] It is essential that the explanation is understandable to the average person, not to professionals.

[34] Articles 13 (2) (f) and 14 (2) (g) of the GDPR.

[35] Article 22 (3) of the GDPR.

[36] Information Commissioner's Office, op. cit., pp. 54-55.

supposed to be supervising the machine does not accept the machine's proposal without reservation, since in such a case there is no human element in the decision-making process and the risk of a possible malfunctioning of the machine is not eliminated, thus, ultimately the decision will be fully automated, meaning that Article 22 applies.

In Section 4 below, I will briefly address certain questions concerning automated decision-making raised in two cases.

3.5 Processing for statistical and scientific purposes

According to Recital (162) of the GDPR, processing for statistical purposes is the collection and processing of personal data for the purpose of calculating statistical results which may be used for various purposes, including scientific research, but which cannot be used to support actions or decisions regarding specific natural persons. Article 89 (2) authorises Member States to provide for derogations from the rights referred to in Articles 15, 16, 18 and 21, subject to safeguards, where such rights are likely to make impossible or seriously impair the achievement of the given purposes and where such derogation is necessary to achieve them.

In view of this, it is possible for Member States to adopt specific rules for the statistical or scientific processing of data collected, for example, for teaching AI models, which do not amend the GDPR but complement it.

3.6 Preliminary questions to be asked

On the basis of Article 25 of the GDPR and as set out in this section, it can be concluded that a data controller[37] should ask itself certain questions when designing the use of an AI-based software, which are briefly summarised below:

a) What is the legitimate purpose of the processing? Care should also be taken to ensure that the use does not turn into processing for purposes incompatible with the original purpose of the processing.
b) What is the legal basis of the processing?
c) How is data accuracy ensured from the data collection phase onwards? Without making sure that the data are accurate, even software with an otherwise excellent algorithm will

[37] Depending on the circumstances, a joint data controller status may arise, or the company developing the AI may be in a data processor's position, thus, it is also necessary for the person/organisation to think about and define their position in advance in the light of the characteristics of the envisaged processing activity.

make wrong decisions, so it is important to take appropriate measures to avoid bias, using sources with reliable information. In particular, the data that is fed into the software must be relevant to and representative of the purpose for which it is being used.

d) How do I comply with the principle of purpose limitation? Only such data may be processed which is necessary for the legitimate purpose for which it is collected, taking into account not only the amount of personal data collected but also the type of personal data.

e) How do I ensure transparency? Data subjects must be properly informed of the processing of their personal data, which is essential because they are in a position to exercise their rights only if they are properly informed.

f) How long do I keep the data? The data controller should properly determine the duration of the processing and integrate erasure and anonymisation settings, whereby, in view of the rapid technological developments, it is essential that the data controller pays particular attention to whether the data can later be re-personalised and, if so, takes the necessary measures.

g) Have I carried out a data protection impact assessment? The data controller has to identify the risks to the rights and freedoms of data subjects posed by the processing, analyse them and take all necessary measures to ensure lawfulness of the processing in an efficient and continuous manner (which necessarily includes the continuous monitoring of the functioning of the software). The availability of the technology alone does not justify the use of AI and a necessity and proportionality test cannot be omitted. In the case of the former, it is necessary to justify why a given legitimate objective cannot be achieved by less invasive means, while in the case of the latter, amongst other things, the risks due to data inaccuracy, model bias and, respectively, potential discriminatory operation must be assessed.

h) Has a testing phase taken place? It is essential that testing is carried out prior to live deployment, so that the data controller can observe and adequately filter out any system deficiencies. Depending on the data entered and the specificities of the algorithm used, the AI may discriminate against natural persons who do not meet certain characteristics, which may not be considered as lawful processing, since such processing would not comply with the principles of lawfulness and fairness (even if the purpose of the processing is lawful, the system collects only the necessary data, the data are accurate and the retention period is appropriate).

i) Will automated decision-making take place? If so, the rights under Article 22 must also be guaranteed. It may be worthwhile anyway to include meaningful human oversight in the process of software operation, so that a particular person can correct a decision that is inappropriate for some reason, for example, if it is discriminatory (in which case the AI would be a tool to assist human decision-making, not a tool to replace it).

j) Do I ensure the rights of data subjects?

k) How can I ensure continuous control over the model and correct its potential errors?

4. EU authority procedures examining the use of AI based on the GDPR

My research has led me to the conclusion that most of the decisions related to AI made so far are linked to the Italian data protection authority (Garante per la Protezione dei Dati Personali, "Garante") and, having consulted with Italian colleagues, I believe this is due to the activities of the Garante itself. Indeed, even before the GDPR became applicable, Garante had already investigated several AI-related issues and imposed measures on data controllers. For example, in 2013, the Garante dealt with the so-called "redditometro", which was a verification tool used by the Italian tax authorities to estimate income. The Italian tax authority created taxpayer profiles by comparing the data provided by taxpayers in their tax returns with data otherwise held by the tax authority and, respectively, inferred from assumptions and estimates based on certain statistics, and from all such data, the authority concluded whether an audit of the taxpayer was necessary because of a presumed risk of tax evasion. The Garante identified various measures to be taken to address the critical points (including ensuring the quality and accuracy of data, the use of an appropriate valuation method such that the taxpayer's true income can only be calculated from actual, documented expenditure, not relying on assumptions based on statistics as to the level of expenditure, and providing taxpayers with adequate information).[38] Also, before 25 May 2018, in 2017, Garante had investigated the installation of "digital billboard" devices (so-called "totems") in a railway station, where a company called Grandi Stazioni Retail S.p.a. had installed digital billboards in the central railway station in Milan. The billboards were equipped with a face detection (not facial recognition) camera. For just a few tenths of a second, the device stored a picture of the face

[38] See https://edri.org/wp-content/uploads/2021/06/Case-studies-Impermissible-AI-biometrics-September-2020.pdf (accessed on 2 September 2023), p. 10, and https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/2765125 (accessed on 2 September 2023).

of the person who passed the billboard in its RAM, and then overwrote the stored image with the next picture taken (the picture was not transmitted to anyone). Based on the picture, the device then spent a few tenths of a second analysing the face image to determine whether the person liked the advertisement (all images were rated on a scale of 1 to 5). The analysis data (serial number of data package, device ID number, time of capture, time spent in front of the billboard, "attention span" of the viewer, gender, age group, distance from the billboard, facial expression) was stored centrally in encrypted form for the purposes of statistical analysis of audience "acceptance" of the advertisement. In its investigation, the Garante considered the measures taken by the company to be adequate, pointing out, *inter alia*, that the system was not a facial recognition system, but only a face detection system, that the legitimate interest of the controller could be the legal basis for the processing, and that the data subjects have to be informed in a simplified way on the spot and in more detail via the website, and that the controller needs to carry out a technical security check of the camera and the local memory at least every six months.[39]

On the other hand, I see the reason for Garante's enhanced AI-related activity in the fact that some members of the authority's management are academics and lawyers who are active in the field of AI and AI-based data processing, thus, this background can also explain why the authority considers it to be of utmost importance to give strong guidance to those who are engaged in a type of data processing that poses increased risks. It is also worth noting that Garante also addressed commitments to monitor AI-related activities in its own semi-annual monitoring plan for 2022, and that the president of the authority attended a hearing before the national Parliament to provide information on the further steps taken by the EU and the safeguards provided by the authority, and announced that the authority would be willing to integrate the authority powers related to AI monitoring. Overall, it is likely that Garante's decisions and statements are intended to draw attention to the undoubtedly close link between privacy and AI and to the justification for vesting the authority with the power to monitor AI rather than creating a separate authority for this purpose.

[39] See https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7496252 (accessed on 2 September 2023).

4.1 The Foodinho case[40]

In July 2021, the Italian data protection authority fined a food delivery network operator, named Foodinho S.r.l. for an amount of EUR 2.6 million for unlawful use of performance evaluation algorithms in connection with its employees. The procedure concerned an investigation into whether the software used by the controller to evaluate the performance of the riders employed was operating lawfully and did not infringe the principle of transparency, in particular, with regard to the automated decision-making it was applying. At the time of the Italian procedure, the company[41] employed around 19,000 riders.

According to the authority's decision, the company operated two systems, the so-called "Excellence system" and the "Jarvis system". The former is an internal scoring system used for the allocation of delivery time slots. Through this system, the company assigns a score to each rider and the riders with a higher score are given priority in the allocation of delivery slots, with the result that “less excellent” riders are excluded from the allocation of the time slots if all available delivery slots are already taken by “better” ones. The score is assigned using an automated mathematical formula based mainly on feedback from customers and partners and delivery ratios. However, negative feedback was given more weight than positive feedback and the system penalised riders who failed to meet certain delivery thresholds. The Jarvis system was used to allocate orders by taking into account data such as geolocation data from a GPS device, food pick-up location, delivery address, special order requirements and vehicle type. Jarvis processed such data to allocate orders in a fully automated way. During the authority procedure, the company failed to clarify exactly how this algorithm worked in conjunction with the Excellence system[42].

[40] https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9677611 (accessed on 14 August 2023).

[41] Lomas, Natasha: Italy's DPA fines Glovo-owned Foodinho $3M, orders changes to algorithmic management of riders, 6 July 2021 (https://techcrunch.com/2021/07/06/italys-dpa-fines-glovo-owned-foodinho-3m-orders-changes-to-algorithmic-management-of-riders/ (accessed on 14 August 2023)).

[42] Milner-Smith, Helena-Cooper, Dan: Italian Supervisory Authority Fines Foodinho Over Its Use of Performance Management Algorithms, 13 July 2021 (https://www.insideprivacy.com/gdpr/italian-supervisory-authority-fines-foodinho-over-its-use-of-performance-management-algorithms/) (accessed on 14 August 2023).

The Garante found that the data controller had breached, *inter alia*, the principles of transparency, data minimisation and storage limitation, Article 13 and the principle of data protection by default and by design.

The company's privacy notice did not contain any information of the fact that automated decision-making was taking place, the logic used, the significance of the processing and the potential consequences of the decision-making for the riders.

The Garante established the breach of Article 25, *i.e.* the principle of data minimisation was violated and access rights within the controller's organisation were in some cases set too broadly.

Article 22 (3) of the GDPR was also breached, as the algorithm operated in a discriminatory manner and the company did not take adequate measures to protect its employees from discriminatory automated decision-making, did not ensure the right to human intervention and the right of the riders to express their views and to contest the decisions taken by the algorithm. The discriminatory nature of the decision-making was manifested in the fact that Foodinho S.r.l. made decisions on the riders based solely on automated decision-making, by analysing their professional performance, their behaviour, their location and movements, and by excluding certain riders from job opportunities on the basis of decisions based on such data, allocating too much weight to the negative assessments.

The authority specifically highlighted that the controller had not verified that the data used by the system were adequate for the intended purposes and did not adopt technical and organisational measures to ensure the accuracy and non-distortion of the system's results.

Accordingly, the authority required the controller, *inter alia*, to (i) provide adequate information to the data subjects, (ii) take measures to protect against discriminatory operation of the system, (iii) ensure the rights of data subjects as set out in Article 22 (3), (iv) take measures to ensure the accuracy of the data and their relevance to the purposes for which they are processed (regularly monitor this), and (v) set appropriate retention periods.

4.2 The Deliveroo case[43]

The Garante also investigated the data processing practice of another company, Deliveroo Italy s.r.l., which also employed food delivery riders, in relation to the processing of the personal data of around 8,000 riders by an algorithm used for work organisation and order allocation among the riders.

Following an investigation into the practices of the data controller, the authority found that the company had not provided transparent information to the riders about the algorithm used to manage the riders' work schedules. Garante added that Deliveroo's software collected a disproportionate amount of personal data on the riders, in breach of the principles of lawfulness, transparency, data minimisation and storage limitation.

The authority also required the data controller to take appropriate measures to protect the rights of the riders, ensure transparency and the accuracy of data when using the algorithm and carry out a data protection impact assessment[44], and imposed a fine of EUR 2.5 million on the company.

[43] See "*Italian Garante Fines Deliveroo 2.5M Euros for Unlawful Processing of Personal Data,*" 5 August 2021 (https://www.huntonprivacyblog.com/2021/08/05/italian-garante-fines-deliveroo-2-5m-euros-for-unlawful-processing-of-personal-data/) (accessed on 15 August 2023).

[44] Separate from this case, there was another case, also in Garante's practice, where, in 2022, the Italian tax authority submitted to Garante for its opinion a data protection impact assessment it had prepared. The aim of the tax authority was to use the AI to try to identify the probabilities, through the analysis of a number of personal data contained in some databases under its processing, of the taxpayers that might be at risk of tax evasion. The Garante authorised the data processing, while stressing that one of the main risks of a stochastic model based on machine learning is the potential errors and biases in the design of the algorithms, and that the measures to be implemented should therefore be adapted to the characteristics of the databases and the analysis models. Among other things, the Garante required the tax authority to monitor the quality of the analytical models and to regularly document the parameters, the activities carried out, the potential critical points and the measures taken to address such critical points with the involvement of the DPO, and to update the impact assessment as necessary. The Garante also required the tax authority to use effective pseudonymisation, to publish an abstract of the impact assessment and to ensure that appropriate human intervention is built into the analysis process and that the staff working with the algorithm are adequately trained to ensure that they are aware of the capabilities and limitations of the algorithmic processes, and to ensure that the staff disregard AI-generated outputs where justified. See https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9808839 (accessed on 2 September 2023).

The algorithm scored the riders, among others, as per the following factors: (i) availability on Friday, Saturday and Sunday evenings, (ii) reliability, and (iii) speed. The authority found that the algorithm was not transparent in its operation, the company could not demonstrate that the algorithm was non-discriminatory, the collection of geolocation data was excessive and that some data were retained for too long.

4.3 The Clearview AI cases

Clearview AI Inc., a US-based company engaged in the operation of a facial recognition software, collected a very large number of photos and geolocation data of natural persons from the Internet[45] and provided access to the database to various investigative authorities.

The company was prosecuted in several EU countries for suspected data breaches, including Italy, France and Greece[46].

4.3.1 Clearview AI and the Italian authority

Following press reports on the software operated by the company and complaints and notifications received by the authority, including complaints received from civil rights organisations, regarding the data processing practices of Clearview AI Inc., the authority identified the following infringements:

- the company processed the personal data in its possession, including biometric and geolocation information, without an adequate legal basis, as the legitimate interest of the company is not an adequate legal basis,
- Clearview AI Inc. violated several principles of the GDPR, such as the principles of transparency, purpose limitation and storage limitation,

[45] According to information available on the Internet, there are currently more than 30 billion photos in use.

[46] Interestingly, in 2021, the Swedish data protection authority fined the Swedish police for an amount of 2.5 million Swedish kronor (about EUR 250,000) for the unlawful use of Clearview AI, among other measures, for breaching Swedish law on the processing of criminal data. See https://edpb.europa.eu/news/national-news/2021/swedish-dpa-police-unlawfully-used-facial-recognition-app_en (accessed on 2 September 2023). It is worth noting that in this case, it was not the GDPR that was applicable, but the specific Swedish law transposing EU Directive 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, given that the processing by the police was for law enforcement purposes.

- the controller failed to provide adequate information to the data subjects as required by Articles 13 to 14 of the GDPR and failed to provide information in accordance with Article 15 at the request of the data subject; and
- the company failed to appoint a representative in the EU.

In its decision of February 2022, the Garante imposed a fine of EUR 20 million on the company for the infringements identified, prohibited further data collection and processing, ordered the deletion of the data processed by the company's facial recognition system, including biometric data, for persons residing in Italy, and ordered the company to appoint a representative in the European Union[47].

As regards the legal basis, the authority argued that since it was not disputed that the consent of the data subjects had not been obtained and given that the conditions referred to in Article 6 (1) (b), (c), (d) and (e) were excluded, it was necessary to examine whether there was a legitimate interest of the controller, implicitly invoked by the company, when suggesting that its activities basically equated to the processing carried out by "Google search"[48].

The authority stresses that there is in principle no general authorisation to re-use and further process personal data made available to the public, the public nature of the data is merely a circumstance that can be one of the factors to be assessed when preparing a legitimate interest assessment[49].

The authority found that the company's legitimate interest was the pursuit of profit in the face of a processing that is particularly invasive in nature, as it consists of the collection of photographic data, combined with additional information that may reveal various aspects of the private life of individuals. These data are biometric data because they are intended to identify a specific individual and relate to a particularly large number of persons, including minors.

---

47 https://edpb.europa.eu/news/national-news/2022/facial-recognition-italian-sa-fines-clearview-ai-eur-20-million_en (accessed on 14 August 2023).

48 https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9751362 (accessed on 14 August 2023).

49 Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 (f) of Directive 95/46/EC (WP217), available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_hu.pdf (accessed on 14 August 2023), p. 16.

The authority specifically drew the attention to the fact that the processing of Clearview AI Inc. also involved sensitive data (biometric data), thus, one of the conditions of Article 9 must be met. In this respect, the authority stressed that the condition in Article 9 (2) (e)[50] was not in itself sufficient to demonstrate compliance, as an appropriate balancing of interests had to be carried out with regard to Article 6 (1) (f).

In the Garante's view, the controller cannot therefore legitimately rely on its legitimate interest as a legal basis for processing and, respectively, the requirements of Article 9 are also infringed.

4.3.2 Clearview AI and the French data protection authority (CNIL)[51]

After May 2020, the CNIL received complaints from individuals about Clearview AI's facial recognition software, following which the authority launched an investigation. In May 2021, Privacy International also warned the CNIL of the company's practices.

The authority first requested the controller to stop the unlawful practice in the territory of France and to deal with the data subject's requests in an appropriate manner, to which request Clearview AI Inc. did not respond. Subsequently, in its decision of October 2022, the CNIL found that there had been unlawful processing of personal data, as the biometric data had been collected and used without a legal basis, and that the rights of data subjects had been infringed, in particular as regards requests for access to and deletion of their data (Articles 12, 15 and 17 of the GDPR) and also imposed a fine of EUR 20 million on the controller, ordering the company to cease the unlawful practice within two months, to stop collecting and processing data of persons residing in France without a legal basis and to delete the data of these persons already collected. It also imposed a fine of EUR 100,000 for each day of delay beyond two months.[52]

As in the Garante's decision, the CNIL stressed that for the processing of personal data to be lawful, processing must be based on one of the legal grounds set out in Article 6 of the GDPR.

---

[50] The prohibition under Article 9 (1) does not apply if *"processing relates to personal data which are manifestly made public by the data subject"*.

[51] In October 2019, the CNIL investigated a facial recognition-based access system installed in schools and found that its use did not comply with the principles of proportionality and data minimisation. See https://www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position (accessed on 2 September 2023).

[52] https://www.cnil.fr/en/facial-recognition-20-million-euros-penalty-against-clearview-ai (accessed on 4 August 2023).

The authority found that the data controller did not seek the consent of the data subjects to collect and use the photographs for the creation and operation of the software. It further indicated that the company had no legitimate interest in collecting and using these data, in particular, in view of the intrusive and mass nature of the company's actions, which allows the retrieval of the images on the Internet of millions of Internet users in France. The data subjects, whose photographs are available on various websites, cannot reasonably expect that their images will be processed by the company for the purpose of developing and operating a facial recognition system which may be used by certain countries for law enforcement purposes. Since the other legal grounds[53] are also not applicable, the use of Clearview AI's facial recognition software has no proper legal basis and the processing carried out is therefore unlawful.

With regard to data subjects' rights, the CNIL noted that the company did not facilitate the exercise of the data subject's right of access because it

- limited the exercise of this right to data collected during the 12-month period preceding the request,
- limited the exercise of this right to twice a year without justification,
- only responded to certain requests if there had been too many requests from the same person,
- the company did not respond or only partially responded to requests for access and erasure.

4.3.3 Clearview AI and the Greek data protection authority

The Greek data protection authority also imposed a fine of EUR 20 million on Clearview AI for the breach of Articles 5 (1) (a), 5 (2), 6, 9, 12, 14, 15 and 27 of the GDPR, following a complaint lodged with the authority. At the same time, the authority ordered the company to comply with the complainant's request for access, prohibited the collection of photographs of data subjects in Greece and ordered the company to delete the personal data of data subjects in Greece that it had collected for the provision of its service[54].

[53] Legal bases under Article 6 (1) (b)-(e) of the GDPR.

[54] https://edpb.europa.eu/news/national-news/2022/hellenic-dpa-fines-clearview-ai-20-million-euros_en (accessed on 2 September 2023).

4.4 The Replica case[55]

Luka, Inc., a US company that developed a "virtual friend" chatbot named Replika, was ordered by the Garante in a decision of February 2023 to immediately cease operating the software in Italy, in particular due to the risks it poses to minors and vulnerable persons.

Concerns had been raised even before about the risks posed to children by such technology, whether one thinks of the exposure to inappropriate content, or the potential for children to become addicted to such software or be encouraged to spend money on, for example, customising their "avatar"[56].

The app is an AI-powered chatbot with a text and voice interface that generates a "virtual friend" users can configure as a friend or partner. Replika is listed on the developer's website and in the two major app stores as a chatbot that can improve users' mood and emotional well-being by helping them understand their thoughts and feelings, help them control stress, relieve anxiety and develop positive thinking.

The Italian authority justified its decision by the following shortcomings:

- the application does not have an appropriate filtering system to check the age of users (in the privacy policy published on the website, the controller has stated that personal data of children under 13 are not collected knowingly, while parents/guardians are encouraged to monitor their children's Internet use and instruct them to never provide personal data without their permission and to contact the platform if they have a good reason to believe that a child under 13 has provided personal data so that such data can be removed from the databases. The app has been classified as suitable for persons over 17 years of age in the two main app stores, while the published terms and conditions mention that children under 13 years of age are not allowed to use the app and that for users under 18 years of age, prior authorisation to use the app must be obtained from their parents or legal guardians),
- the program only asks users to enter their name, email address and gender,

[55] https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9852214#english (accessed on 14 August 2023).

[56] Lomas, Natasha: Replika, a 'virtual friendship' AI chatbot, hit with data ban in Italy over child safety, 3 February 2023 (https://techcrunch.com/2023/02/03/replika-italy-data-processing-ban/) (accessed on 13 August 2023).

- no blocking mechanisms are triggered even if the user explicitly states that he/she is a minor,
- the privacy notice does not contain information on the essential elements of the processing, in particular the processing of children's personal data, and, thus, violates the principle of transparency,
- the legal basis for the processing cannot be determined, since in the case of children it can be excluded that the legal basis for the processing is the performance of a contract with the data subject as children have no legal capacity under Italian law,
- the software generates responses for children that are not appropriate for them (*e.g.* some answers are of sexual contents).

On the basis of the above, the Garante found that the controller had violated Articles 5, 6, 8, 9 and 25 of the GDPR.

4.5 The Budapest Bank case[57]

In this case, the Hungarian data protection authority (NAIH) investigated the processing of data by artificial intelligence through the use of machine learning-based AI software for voice recording analysis by Budapest Bank. The authority found violations of several provisions[58] and imposed a fine of HUF 250 million[59] on the controller.

The bank used the AI-based software to automatically analyse the audio recording of customer service calls and, based on the results of the analysis, determine which dissatisfied customers needed to be called back. The software automatically analysed the emotional state of both the calling customer/concerned party and the customer service employee, as well as other characteristics of the conversation. The authority examined whether the bank's data processing activities in relation to the automatic analysis of recorded customer service calls, the listening to the recordings and the recall of certain data subjects complied with data protection requirements, including the obligation to provide adequate information to data subjects of the processing.

[57] NAIH-85-3/2022, former case number NAIH-7350/2021.

[58] GDPR Articles 5 (1) (a) and (b), 6 (1), 6 (4), 12 (1), 13, 21 (1) and (2), 24 (1), 25 (1) and (2).

[59] This amount, calculated at an exchange rate of HUF 383 to the EUR, is equivalent to about EUR 653,000.

According to the bank, the software analysed and ranked the calls based on the characteristics that were entered, which the bank was not aware of[60], and the calls were randomly played back. The system was operated to "control call quality", "prevent complaints and customer churn" and "increase efficiency"[61].

The authority found that by ranking the calls, the software essentially suggested which person should be called back. The decision to recall was made by the bank's employees. The purpose of the recall was to address customer dissatisfaction, not to address a specific complaint.

The authority found that the privacy statement contained only general information on call analysis[62], did not describe the method and characteristics of voice analysis, and it referred to quality assurance and complaint prevention, not to the handling of dissatisfaction.

The NAIH found that the data controller did not inform the data subjects about what data were being processed, how they were being processed and of the fact that their emotional reactions were being analysed. The authority added that out of the elements of information to be provided as per Article 13, only the legal basis was named by the controller and the purpose of the processing was not fully specified.

In the part of the decision dealing with the bank's legitimate interest assessment, the authority stresses that, as the use of AI is typically difficult to make transparent, it is also *"particularly important to pay attention – not only on paper, but also when it comes to actual implementation – to the use of AI during processing if the controller is to comply with the transparency and accountability requirements of the GDPR. This goes beyond the default level of expectation for an average risk processing and, taking into account the risk-based approach under Articles 24 and 25 of the GDPR, this difficulty should be taken into account when the controller decides*

[60] According to the bank's statement, *"[...] The software analyses the voice recording according to [...] criteria, which are trade secrets of the developer. The developer named as examples the speed of speech, volume, pitch, length of pauses in speech. The analysis does not result in a profile, but the recordings are ranked daily by the system. The ranking is based on the conclusion that the caller, although not putting forward a formal complaint, was dissatisfied with the service, based on the aspects examined."*

[61] See Decision, p. 3.

[62] The bank *"carries out profiling based on its legitimate interest for quality assurance and complaint prevention purposes and selects those calls by automatic decision where a more highly qualified bank employee will resolve the problem or complaint raised in the telephone conversation by means of a callback"*, decision, pp. 20 and 25.

when and for what purpose it wishes to use AI and how to ensure transparency in this respect."[63]

In my opinion, the few lines quoted above could be considered as a brief summary of the essence of the decision, because, in fact, "all" other obligations follow from Article 25, they can be directly deduced from it. At the same time, the NAIH refers to the Joint Opinion 5/2021 of the European Data Protection Board and the European Data Protection Supervisor[64] on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), which states that the use of AI for the purposes of analysing the emotions of natural persons is undesirable and should be prohibited, subject to a few exceptions.

The authority found that the controller's legitimate interest could not be used as a legal basis, given that the balancing of interests only included the reasons why the bank needed the data (processing), but the data subject's side was not examined by the bank and, thus, the different interests were not weighed, *i.e.* no real balancing of interests was carried out.

Examining the rights of data subjects, the NAIH found that the bank had not made sure that the data subjects could exercise the right to object[65]. Also, due to the lack of adequate information, the callers could not suspect that their voice would be analysed by the bank, which in itself results in a violation of the data subject's rights, since if the data subject is not aware of a processing, he/she cannot exercise his/her rights in relation to it. On the other hand, the fact that a customer calls a bank does not imply that he/she can expect his/her voice to be analysed and he/she can potentially be recalled because the analytical software may have indicated that he/she was dissatisfied.

[63] See decision, p. 26.

[64] https://edpb.europa.eu/system/files/2021-10/edpb-edps_joint_opinion_ai_regulation_hu.pdf (accessed on 19 July 2023).

[65] It is also interesting in this case that no automated decision-making as per Article 22 of the GDPR had taken place, because, although, the decision not to recall customers not recommended for recall was fully automated, there was no legal effect or similarly significant effect for such customers, while in the case of the customers recommended for recall, the decision to recall was ultimately made by a bank employee, meaning that in the customer's case, Article 22 did not apply. At the same time, the control of employees was also the result of human decision, thus, in the employees' case, no fully automated decision-making as per Article 22 took place either.

4.6 The ChatGPT case

There had been numerous news reports about the Garante's decision in March this year, which temporarily banned the use of ChatGPT in Italy, but the specific details were less clear, with the press mainly picking up on the fact that ChatGPT is banned in Italy. Below is a summary of the "ChatGPT case".

The case was preceded by a data breach reported on 20 March this year, which affected ChatGPT users' conversations and the payment details of the service's subscribers[66].

In its decision of 30 March 2023[67], the Garante, indicating that AI-based software based on large language models is also subject to the EU's data protection legislation, stated that

- the operator of ChatGPT, a US company named OpenAI, LLC, had not provided adequate information on data processing to the users of the software and, respectively, to the natural persons whose personal data was collected by the controller and used for the purpose of teaching the software,
- there was no proper legal basis for the collection and processing of personal data for the purpose of teaching the algorithms used for the operation of ChatGPT,
- the processing of the personal data of the data subjects did not comply with the principle of accuracy, given that the information provided by ChatGPT was not always accurate; and
- the age of the users was not verified by the data controller in relation to the service, which was reserved for persons aged 13 years and over according to the terms and conditions published by OpenAI, LLC, indicating that children under 13 years of age were exposed to responses that were not appropriate to their level of development and self-awareness, due to the lack of filters.

In its decision, the Garante, considering that the processing of data by ChatGPT infringes Articles 5, 6, 8, 13 and 25 of the GDPR, ordered the temporary restriction of processing with immediate effect of the personal data of natural persons residing in Italy. At the same time, the

[66] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9870847#english (accessed on 4 August 2023).

[67] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9870832 (accessed on 4 August 2023).

Garante requested the controller to communicate, within 20 days, the measures taken to implement the authority provisions and to provide any information it considers useful to justify the breaches identified by the authority.

OpenAI, LLC is not established in the EU, thus, each EU data protection authority has the right to act independently against OpenAI, LLC, which could undermine the development of a consistent EU practice, as it cannot be ruled out that the different EU data protection authorities would view certain aspects of ChatGPT's data processing in a different way. Sensing this, the Garante took the initiative to have the European Data Protection Board address the issue of data processing by ChatGPT, following which a special working group was set up within the European Data Protection Board. The details of the working group's work are currently not known.

Following the issuance of the above-mentioned order, after a meeting between OpenAI, LLC and the authority, the Garante published a notice on 12 April[68] setting out the obligations imposed the data controller had to comply with in order to lift the ban. The Garante provided that

- the data controller must prepare and make available on its website a privacy notice explaining the features and rationale of the processing necessary for the operation of ChatGPT and the rights of data subjects (for both users and non-users),
- the information notice must be easily accessible and positioned so that it can be read before registering for the service,
- registered users should receive a warning when accessing the service, after reactivating it, when they have to pass an age filter that filters out underage users based on the age they enter,
- regarding the legal basis of the processing of users' personal data for the purpose of teaching the algorithms, OpenAI, LLC must delete all references to the performance of the contract and base the processing on the data subject's consent or on the legitimate interest of the controller (or a third party), in accordance with the principle of accountability,

[68] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9874751 (accessed on 4 August 2023).

- the controller must allow data subjects, including non-users, to have their personal data erroneously processed by the service rectified or, where rectification is technically impossible, erased. The controller should provide readily accessible means for non-users to exercise their right to object to the processing of their personal data used for the operation of the algorithms, which right must be available also to users where the legal basis for the processing of their data is based on legitimate interest,
- Open AI, LLC must immediately implement an age verification system for registration to the service, submit a plan and implement the solution by 30 September 2023 to filter out users under 13 years of age and users between 13 and 18 years of age without parental consent,
- by 15 May, OpenAI, LLC must, in agreement with the authority, carry out an information campaign on radio, television, newspapers and the Internet to inform individuals of the use of their personal data for the purpose of teaching the algorithms.

The authority added that it would continue to investigate possible breaches of the legislation in force and might decide to take further action if it proved necessary.

In its notice of 28 April[69], the Garante disclosed that OpenAI, LLC notified the authority that (i) it had prepared and published on its website a privacy notice for users and non-users describing the measures taken to process personal data for the purpose of teaching the algorithms and drawing everyone's attention to the right to opt out of the processing, (ii) it had prepared a privacy notice for users, which it made available on the registration page prior to registering for the service, (iii) it ensured all European individuals, including non-users, the right to opt-out of the processing of their personal data for the purpose of teaching algorithms through an online, easily accessible form, (iv) it had introduced a welcome page for the relaunch of the service in Italy, which includes a link to the new privacy notice for users, and a privacy notice for non-users on the processing of their personal data for the purpose of teaching the algorithms, (v) it had introduced mechanisms to allow data subjects to request the erasure of information deemed inaccurate, while indicating that it was not technically feasible to rectify inaccuracies at that stage, (vi) it had made clear in the privacy notice that it would continue to process certain personal data to enable it to provide its services on a contractual

[69] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9881490 (accessed on 4 August 2023).

basis, and to process users' personal data on the basis of its legitimate interest in teaching algorithms (at the same time, users were allowed to request that their personal data not be processed for the purpose of teaching the algorithm), (vii) it had placed a separate button on the registration page of the service dedicated to registered Italian users, asking them to confirm that they have reached the age of 18 before access or the age of 13 and that their parents or guardians have given their consent to the processing of the data, and a request for information on the date of birth was included on the registration page of the service to prevent access by users under 13 years of age, just like a request for confirmation of consent by parents or guardians for users between 13 and 18 years of age.

The privacy policy for users of ChatGPT[70] and the one for non-users[71] raise, in my opinion, several data protection issues:

a) The privacy policy to users explicitly points out, with regard to data accuracy, that *"services like ChatGPT generate responses by reading a user's request and, in response, predicting the words most likely to appear next. In some cases, the words most likely to appear next may not be the most factually accurate. For this reason, you should not rely on the factual accuracy of output from our models. If you notice that ChatGPT output contains factually inaccurate information about you and you would like us to correct the inaccuracy, you may submit a correction request through privacy.openai.com or to dsar@openai.com. Given the technical complexity of how our models work, we may not be able to correct the inaccuracy in every instance. In that case, you may request that we remove your Personal Information from ChatGPT's output by filling out this form."*[72]

The question is whether the above information and the certainly advanced technical background behind it meet the requirements of the GDPR, in particular, the principle of accuracy and the safeguarding of data subjects' rights, in this case, the right to rectification. The *"right to rectification is closely linked to the principle of accuracy"*[73] and *"data*

[70] https://openai.com/policies/privacy-policy (accessed on 4 August 2023).

[71] https://help.openai.com/en/articles/7842364-how-chatgpt-and-our-language-models-are-developed (accessed on 4 August 2023).

[72] https://openai.com/policies/privacy-policy (accessed on 4 August 2023) See clause 4 of the privacy notice.

[73] Péterfalvi Attila-Révész Balázs-Buzás Péter (eds.): *GDPR.* Wolters Kluwer, Budapest, 2021, electronic version Section 7.2.1.2.

controllers must take measures to ensure that the information processed is accurate at the time of recording personal data, which is complemented by the right of the data subject to have his/her data rectified"[74].

Article 5 (1) (d) of the GDPR states that *"every reasonable steps must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay"*. In my view, the above information may comply with this, while, at the same time, it seems appropriate to develop a position which, together with the accountability for compliance, takes a constructive approach to the use of AI, *i.e.* a sufficiently flexible interpretation of the GDPR rules is accepted without breaching data protection rules. I believe that if it is indeed technically not feasible to ensure the right of rectification[75] in a reasonably justifiable way (the reasons why it is not feasible should be specifically examined), then erasure of the data seems a sufficient alternative.

b) according to Section 8 of the privacy policy, the data will be kept by the controller for as long as it is necessary to provide the service to the data subject or for other legitimate business purposes, such as dispute resolution, security reasons or to comply with legal obligations. The notice adds that the period of data retention depends on a number of factors, such as the amount, nature and sensitivity of the data, *etc.*

It is questionable to what extent such a generally formulated information can comply with data protection requirements, in particular, the principles of transparency and storage limitation. In my view, it could be justified that more specific and precise information would be necessary, for example, if the controller refers to a legal obligation, it could be expected to specify the concrete legal obligation and to explain how the retention period depends on the factors it lists.

c) What is perhaps one of the most interesting questions is how to ensure that the personal data collected so far have been lawfully processed from the moment they were obtained. According to the non-users' privacy policy[76], the personal data collected for the purpose of teaching ChatGPT is collected from three sources, which are as follows: (i) publicly available Internet content, (ii) data obtained from third parties and (iii) data provided

[74] Péterfalvi Attila-Révész Balázs-Buzás Péter (eds.): op. cit., point 7.2.1.2.

[75] In my view, the reasons why it is not technically feasible to rectify data should be examined on a case-by-case basis and, depending on the answer, there may be situations where it is acceptable that the controller cannot handle rectification, only erasure.

[76] The document is entitled *"How ChatGPT and Our Language Models Are Developed"*.

by users and human trainers. The purpose of the policy is to provide information on the data collected from the Internet.

According to the policy, OpenAI uses only publicly available information that is freely available on the Internet – for example, it does not look for information "behind paywalls" or from the "dark web" – and applies filters and removes information that it does not want its software to learn from or see in responses, such as hate speech, adult content, sites that aggregate primarily personal information and spam. Otherwise, the information is used by the data controller to train its models. The policy also states that much of the data on the Internet relates to people, so the data used for teaching incidentally contains personal data too, and stresses that the controller does not actively seek personal data for teaching language models.

In particular, the privacy policy points out that the controller does not and will not use any personal data contained in the information used to teach the model to profile or contact anyone, advertise to, or try to sell to people anything.

In addition, the policy also contains that large language models have a number of uses that bring significant benefits and are already helping people in areas such as content creation, improving customer service, software development, tailoring education, supporting scientific research, and that these benefits cannot be achieved without using the large amount of information needed to teach the models. The controller also emphasises that the use of the information used to teach the model is not intended to have a negative impact on individuals and that the sources of the information used for teaching are publicly available anyway; and in view of all these aspects, the collection of personal data contained in the information used for teaching is based on a legitimate interest under the GDPR, and finally, the controller also states that it has carried out a data protection impact assessment to ensure compliance.

In the "*How does the development of ChatGPT comply with privacy laws?*" section of the policy, OpenAI seeks to justify its lawful use of people's data by arguing that a) it intended its chatbot to be a useful program, b) it had no choice since creating an AI technology requires a huge amount of data, and c) it did not want the program to have any negative impact on individuals[77].

[77] Lomas, Natasha: ChatGPT resumes service in Italy after adding privacy disclosures and controls, 28 April 2023 (https://techcrunch.com/2023/04/28/chatgpt-resumes-in-italy/?guccounter=1) (accessed on 4 September 2023).

In my view, it is not clear how OpenAI, LLC can demonstrate that the processing of data previously collected from the Internet was lawful at the time it was obtained. If the data controller cannot prove this, erasure of the data can be ordered, which is in itself a very serious sanction, since the very essence of the language model is that it learns and evolves from the data fed into it. If the learning process had to be restarted, this could cause serious difficulties for OpenAI and certainly much valuable learning experience would be lost.

4.6.1 Lessons learned from the ChatGPT case so far

In the case of ChatGPT, in my view, it seems possible that the data controller may have failed to apply, or may have inadequately applied, the principle of privacy by design and by default when it started collecting publicly available information (including a large amount of personal data) on/from the Internet and using it to teach an AI-based large language model.

There is no doubt that the controller, the developer of the software, needs to act in good faith when designing a processing activity, but this alone is not sufficient for the processing to be lawful. The principle of data protection by design and by default no doubt requires compliance with the principles and requirements of the GDPR already at the design stage of data processing, including the identification and assessment of risks, the adoption of appropriate technical and organisational measures proportionate to the risks, and the incorporation of safeguards to ensure the continuous and effective protection of the rights of data subjects; all of which can certainly not be met by the controller by stating that it did not intend to do any harm and that it was motivated by good intentions.

Taking into account the conditions set out in clauses (a)-(j) in Section 3.6 above is even more important when processing is done by using a large language model, which may present risks that would not be present in case of a technically less sophisticated processing.

A fundamental requirement of the GDPR is that whenever personal data are processed, there must be an adequate legal basis for the processing[78]. Ensuring that there is an adequate legal basis is the obligation of the controller, and its existence is a necessary but not a sufficient condition of lawful processing. This is no and cannot be different when artificial intelligence is used to process personal data.

[78] Article 6 of the GDPR.

Generally speaking, the legal basis for processing by a large language model created by a private company for the processing of personal data is likely to be either the consent of the data subject or the legitimate interest of the controller (and/or a third party) (except, in the latter case, if, for example, the data subject is a child). This is confirmed by the opinion of Lilian Edwards, a lecturer at Newcastle University, who argues that in the case of ChatGPT there are essentially two options: obtain the data subject's consent (which OpenAI has failed to do) or claim that the controller has a legitimate interest in processing the data, which is very difficult[79].

In the above-mentioned Garante order, OpenAI, LLC was ordered to delete the reference to the performance of the contract and to base the processing on the data subject's consent or on legitimate interest as defined in the GDPR. The latter may only be the legitimate interest of the controller or a third party.

As stated in OpenAI, LLC's privacy policy on the processing of personal data collected from the Internet and used to teach the model, the controller has a legitimate interest in the use of personal data to teach the model. Interestingly, the policy does not specify the legitimate interest itself (although, it should under the GDPR[80]), but merely names legitimate interest by reference to the fact that the software is useful, is not intended to harm anyone, the data collected had been publicly available before it was collected and the data is not used for any purpose other than teaching the model.

In my view, it is highly questionable whether this is sufficient for providing an adequate legal basis since the mere fact that the personal data is publicly available on the Internet does not mean that it can be freely processed without complying with the relevant data protection rules, nor does the mere fact that the processing is not intended to have any negative effect on individuals or that the controller does not use the data for contacting the data subjects, for example, for advertising purposes, seem sufficient to demonstrate lawfulness since doing so would in itself mean unlawful processing, and the fact that the controller does not unlawfully process data for purposes other than the original purpose does not imply that the processing for the original purpose can only be lawful.

[79] Burgess, Matt: ChatGPT Has a Big Privacy Problem, Italy's recent ban of Open AI's generative text tool may just be the beginning of ChatGPT's regulatory woes, 4 April 2023 (https://www.wired.com/story/italy-ban-chatgpt-privacy-gdpr/) (accessed on 14 August 2023).

[80] Articles 13 (1) (d) and 14 (2) (b) of the GDPR. In this case, the latter legal provision applies, given that the personal data were not obtained directly from the data subject but from the Internet.

At the same time, even if legitimate interest was duly proven for the future, it is questionable how the controller could demonstrate that the processing of personal data collected previously – *i.e.* before the start of the processing based on legitimate interest – is lawful.

As Tobias Judin, head of international at the Norwegian data protection authority put it: *"If the business model has just been to scrape the internet for whatever you could find, then there might be a really significant issue here.",* adding that if a model relies on data that may be collected unlawfully, it raises questions about whether anyone can use such tools legally[81].

Here again, it is confirmed that it is important to think about and plan the processing in due time, namely, before starting the processing. This is because on the one hand, one cannot undo things that have occurred, and on the other hand, it is not possible to subsequently provide a legal basis for the processing of personal data that was originally collected unlawfully.

5. Summary

Based on the decisions outlined above, I will summarise below the main lessons for data controllers and processors, and then briefly address whether I believe that the GDPR needs to be amended with a view to taking account of the new and evolving technology AI means.

5.1 Lessons learned from public authority decisions concerning AI

Some of the provisions of the GDPR are closely interlinked, and many of them cannot be separated from the others because they form a coherent set of rules together. One could think of, for example, what the above-mentioned cases have shown excellently, namely, that from these few cases alone, lessons can be drawn that are also applicable to any AI-based data processing, which are briefly summarised below:

- when developing algorithms, one must take into account the principles (*e.g.* transparency, data minimisation, accuracy), ensure that data subjects' rights can be exercised, identify risks and take appropriate measures to address them. If the developer is in a data processor's status, then, despite the fact that Article 25 contains obligations applicable to the controller, it is advisable to take into account the principle of data protection by design and by default, because the customer (data controller) buying the product is obliged to properly educate itself about the software in advance and can only use a program that complies with data protection law (in other words, in the case of data

[81] Burgess, Matt: op. cit.

controllers acting in a prudent manner, the developer who is a data processor will only be able to sell the software if it can prove that the software was designed to comply with, *inter alia*, Article 25),

- a data protection impact assessment needs to be carried out, which in itself can help to assess the likelihood and severity/impact of the risks. Although, this obligation is also vested with the data controller, the software developer may prepare a data protection impact assessment for its product in order to demonstrate compliance to its customers,
- when it comes to the planned application of a machine learning-based AI, special attention should be paid to ensure that the data collected are adequate and relevant to the purpose, and that only the necessary data are collected and that they are kept only for the necessary period of time,
- it is important to (also) provide clear information on how the algorithm works (in the case of solely automated decision-making, information must be provided also on the logic used, the significance of the processing carried out and the envisaged consequences for the data subject),
- continuous monitoring of the "output" of the algorithm is necessary to prevent and correct potential errors, biases and discriminatory decisions.

All of the above requirements can be derived from Article 25 of the GDPR, as the requirement therein constitutes compliance with Articles 5, 6-9, 12-22, 24, 32 and 35-36, among others.

5.2 Conclusions

Based on the analysis of data processing through the use of AI from the perspective of the GDPR and practice, the aim of this thesis was to answer the question whether the GDPR contains rules compatible with the use of AI or whether there are rules that should be adapted.

Undoubtedly, one can feel a tension between the requirements of the GDPR (in particular, the principles of transparency, data minimisation, accuracy and storage limitation), compliance with such requirements and the specificities of the way AI models work, which means that data controllers must take special caution before engaging in data processing through an AI-based model, *i.e.* already at the design stage.

At the same time, there can be little doubt that anyone would be of the opinion that some or all of the principles of the GDPR should be sacrificed in order to allow more room for

technological development. Who would agree that data processing by AI means should be less fair or less transparent? Or that the principle of purpose limitation is not so important in the case of AI-based processing, or that data may be inaccurate, storage limitation should not be taken as seriously or the controller should not act with the level of care as required by Article 25 when it comes to AI-based processing? These are all legitimate questions, but if they are put in the context of the fact that an advanced and less known technology may pose increased risks to data subjects precisely because of its characteristics and capabilities, the relevance of these questions becomes even more apparent, since if the answer was in the affirmative, it would mean that we would apply a lower level of protection to a data processing with increased risks, which, in my view, would not be the right approach to take[82].

In my opinion, it is important to pay attention to the proper application of the existing rules of the GDPR, especially on the part of data controllers (processors), but it is equally important that authorities and courts interpret the given rule within the framework set by the GDPR with sufficient reasonableness, while, at the same time, reducing transparency and security as well as *"[t]he erosion of data subjects' rights cannot be the aim and result of progress."*[83]

As the Research Service of the European Parliament concluded in a study, *"there are ways to interpret, apply, and develop the data protection principles that are consistent with the beneficial use of AI and big data."*[84].

In agreement with the Research Service of the European Parliament, it is desirable and important that the European Data Protection Board and the individual authorities issue guidance on the use of AI, which can provide useful information for data controllers and

[82] The High Level Expert Group on Artificial Intelligence set up by the European Commission also stresses the importance of the following four ethical principles for the use of trusted AI: (i) respect for human autonomy, (ii) avoidance of harm, (iii) fairness, (iv) transparency, provision of adequate information.
The Information Commissioner's Office also stresses that technology may be new, but the principles of data processing remain the same, and it is important to act from the outset in accordance with the principle of privacy by design and by default, which is not optional as the law itself requires it (https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/04/generative-ai-eight-questions-that-developers-and-users-need-to-ask/ (accessed on 19 August 2023).

[83] See Budapest Bank decision, p. 29.

[84] The impact of the General Data Protection Regulation (GDPR) on artificial intelligence, Study Panel for the Future of Science and Technology, EPRS | European Parliamentary Research Service, Scientific Foresight Unit (STOA), PE 641.530 - June 2020, Executive summary, p. II.

processors and which gives information on how to use certain AI technologies in line with the law that is more concrete than the provisions of the GDPR[85]. While it is undisputed that it is the responsibility of data controllers and processors to set up data processing in a compliant way, such guidelines would ultimately be in the interest of all, including data subjects and the society at large, taking into account that there can be many beneficial uses of AI.

In conclusion, in my view, there is no need to amend the GDPR with respect to AI, but at the same time, in addition to issuing authority guidance as mentioned above, it seems reasonable that Member States take advantage of the authorisation referred to in Section 3.5 above regarding the use of data collected by AI models for scientific research and statistical purposes, thereby facilitating technological development and the use of AI for the benefit of all.

The text of this thesis was finalised on 8 September 2023, thus, developments after that date are not addressed herein.

[85] The impact of the General Data Protection Regulation (GDPR) on artificial intelligence, op. cit., Executive summary, p. III.