Journal scientific and applied research, vol. 28, 2025
International Journal

Original Contribution

ISSN 1314-6289 (Print)
ISSN 2815-4622 (Online)

HOW GDPR TREATS AUTOMATED DECISION-MAKING

Iliana K. Simeonova

DEPARTMENT OF COMMUNICATION AND COMPUTER ENGINEERING AND SECURITY TECHNOLOGIES, FACULTY OF TECHNICAL SCIENCES, KONSTANTIN PRESLAVSKY UNIVERSITY OF SHUMEN, SHUMEN 9712,115, UNIVERSITETSKA STR., E-MAIL: i.simeonova@shu.bg

ABSTRACT: *This article examines how the General Data Protection Regulation (GDPR) regulates automated decision-making, including profiling, in the context of personal data processing. It analyzes the main provisions of Article 22 of the Regulation, as well as the conditions under which fully automated decisions that produce legal effects or significantly affect data subjects are permitted. The article highlights the rights of data subjects – the right to human intervention, the right to express their point of view, and the right to contest the decision – along with the responsibilities of data controllers. Practical examples and commentary are included, focusing on the application of these rules in the context of modern technologies such as algorithmic profiling, artificial intelligence, and machine learning.*

KEY WORDS: *GDPR, Automated decision-making, Profiling, Article 22, Personal data, Artificial intelligence, Data subject rights, Data protection, Algorithms, Transparency.*

1. Introduction

In the context of increasing digitalization and widespread implementation of technologies based on artificial intelligence and algorithmic models, the issue of automated decision-making is becoming crucial both for business and for the protection of fundamental human rights. Regulation (EU) 2016/679 on the protection of personal data (GDPR) is one of the most significant pieces of legislation in the current legal framework of the European Union, regulating the processing of personal data and introducing specific restrictions on automated individual decision-making, including profiling.

This report aims to examine how the GDPR defines, restricts, and regulates automated decision-making, as well as to analyze the practical challenges organizations face in implementing the relevant provisions. The focus is on Article 22 of the Regulation, which formulates the principle of prohibiting decisions based solely on automated processing and provides for rights for data subjects, ensuring human intervention and transparency.

2. Overview of the general data protection regulation (GDPR)

Regulation (EU) 2016/679, which entered into force on May 25, 2018, aims to strengthen and harmonize the protection of individuals' personal data within the European Union and to enhance individuals' control over their own data. Among the fundamental principles laid down in the Regulation are the principles of lawfulness, fairness, and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality; and accountability of controllers and processors.

The GDPR establishes a number of subjective rights for individuals, including the right of access, the right to rectification and erasure ("right to be forgotten"), the right to restriction of processing, the right to data portability, and the right to object. In this context, the right of the data subject not to be subject to a decision based solely on automated processing deserves special attention.

2.1. Main objectives and principles of the Regulation.

The main objective of the GDPR is to ensure a high level of protection of individuals' personal data and to increase trust in the digital economy. The Regulation introduces a strict set of principles that form the core of the legal regime for data protection and guide all personal data processing activities. Among them, the following are of particular importance:

Principle of transparency, fairness, and lawfulness: Personal data must be processed in a manner that is transparent to the data subject. This includes clear and understandable information about the purposes, scope, and legal basis of the processing (Article 5, §1, point "a"). Transparency is achieved through prior notification, the use of accessible language, and the provision of information about the rights of individuals.

Purpose limitation principle: Data may only be collected for specific, explicitly stated and legitimate purposes and may not be further processed in a manner incompatible with those purposes (Art. 5, §1, item "b").

Principle of data minimization: Personal data processed must be adequate, relevant, and limited to what is necessary in relation to the purposes of the processing (Article 5, §1, item "c"). This requires careful consideration of the volume and type of data collected.

Accuracy principle: Data must be accurate and, where necessary, kept up to date. All reasonable steps must be taken to ensure that inaccurate data is deleted or corrected in a timely manner (Art. 5, §1, (d)).

Principle of storage limitation: Data must be stored in a form that allows identification of data subjects for no longer than is necessary for the purposes for which it is processed (Art. 5, §1, item "f").

Accountability principle: Personal data controllers are responsible for complying with the principles and must be able to demonstrate compliance with them (Art. 5, §2). This is a new, essential feature of the GDPR, which requires a proactive approach to data management.

2.2. Key rights of data subjects.

The GDPR significantly expands the scope and depth of the rights granted to individuals, known as data subjects. These rights are a tool for exercising control over their personal data and include:

According to Article 15 Right of access – Individuals have the right to obtain confirmation as to whether their personal data is being processed, as well as access to the data itself and information about how it is being processed.

According to Article 16 Right to rectification - Data subjects may request the correction of inaccurate personal data or the completion of incomplete data.

According to Article 17 Right to erasure ("right to be forgotten") -Under certain conditions (e.g., if the basis for processing no longer applies), data subjects may request the erasure of their personal data.

According to Article 18 Right to restriction of processing - Allows for the temporary suspension of processing in the event of a dispute regarding the accuracy, lawfulness, or necessity of processing.

According to Article 20 Right to data portability - Data subjects may receive their personal data in a structured, commonly used, and machine-readable format and transfer it to another controller.

According to Article 21 Right to object - Allows the data subject to object to the processing of data based on legitimate interest or the performance of a task in the public interest, including profiling.

According to Article 22 Rights related to automated decision-making, including profiling - Individuals have the right not to be subject to a decision based solely on automated processing which produces legal effects or significantly affects them.

2.3. The role of controllers and processors of personal data.

A data controller is any natural or legal person, public authority or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data (Article 4, point 7). Controllers have the primary responsibility for complying with the principles of the GDPR, including the obligations to ensure transparency, security [2,3] and accountability.

The main obligations of the controller include:

- Conducting impact assessments (DPIA) for high-risk processing;
- Appointing a data protection officer (DPO), where necessary;
- Ensuring data protection by design and by default;
- Keeping records of processing activities.

A data processor is a person or organization that processes personal data on behalf of and on the instructions of the controller (Article 4, point 8). Although acting on an assignment, the processor also has specific obligations, including:

- Compliance with the contractual terms and conditions established in accordance with Article 28 of the Regulation;

- Ensuring appropriate technical and organizational measures to protect data;
- Assisting the controller in exercising the rights of data subjects.

The cooperation between the controller and the processor must be regulated by a written contract that clearly distinguishes the responsibilities and obligations of each party. In the event of a breach, the GDPR provides for the possibility of joint and several liabilities in the event of insufficient distinction or non-compliance with obligations.

The GDPR represents a quantum leap in the evolution of European data protection law. With its clearly defined principles, strong rights for subjects and strict obligations for organizations, the Regulation creates a stable and predictable.

3. Automated decision-making and profiling: legal framework and practical dimensions

Article 22 of the GDPR is the key provision governing automated individual decision-making. As defined in Article 4(4), profiling is any form of automated processing of personal data, consisting of the processing of personal data to evaluate certain personal aspects relating to a natural person, such as analysis or prediction of aspects concerning his/her performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Automated decision-making covers situations where a decision that produces legal consequences for a natural person or similarly significantly affects them is taken exclusively by automated means, without human intervention. Typical examples of such decisions are the automatic approval or refusal of a loan, the algorithmic selection of job candidates or personalized offers based on profiling.

With the development of digital technologies, machine learning and big data, the possibilities for automated processing of personal data have increased significantly. This has led to increased interest and concern about the way algorithms make decisions that affect the rights and freedoms of natural persons. In response to these challenges, the General Data Protection Regulation (GDPR) establishes specific provisions governing automated individual decision-making, including profiling, as separate but interrelated forms of processing of personal data.

3.1. Automated individual decision-making.

According to Art. 22 of Regulation (EU) 2016/679, the data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or significantly affects him or her.

Interpretation of the key elements of Art. 22: *"Automated"* - the decision must be taken without human intervention, i.e. without a person actually reviewing and/or confirming the result of the algorithm.

"Produces legal effects or significantly affects him or her" - this includes situations such as refusal of credit, refusal of insurance, automatic rejection of a job application, change of tariff based on user behavior, etc.

Exceptions from Art. 22, §2 - Automated decision-making is permissible in the following cases:

- ✓ Necessity for the conclusion or performance of a contract;
- ✓ Explicit consent of the subject;
- ✓ Authorised by EU or national law with appropriate safeguards;

In these cases, appropriate measures must be implemented to protect the rights of the subject, including the possibility of human intervention, expression of views and appeal against the decision.

3.2. Distinction between Profiling and Automated Decision-Making

Profiling.

Defined in Article 4(4) of the GDPR, profiling is: "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements."

Profiling in itself is not prohibited by the GDPR. However, when it results in automated decisions that have significant consequences, it falls within the scope of **Article 22**.

Automated individual decision-making

This is a broader concept that may include profiling, but it necessarily ends with a decision made without human intervention, which significantly affects the individual (table 1).

Table 1 Key Differences

Criterion	Profiling	Automated Decision
Purpose	Evaluation, analysis, or prediction of characteristics	Making a specific decision
Human Involvement	May include human review	No human involvement
Legal Effect/Impact	Does not always lead to direct impact	Always has a significant impact
Example	Segmenting users based on interests	Automatically denied credit application

3.3. Practical Examples

The following examples illustrate how automated decision-making and profiling are applied in practice:

✓ **Credit scoring:** Financial institutions use algorithms to assess a client’s risk profile based on factors such as payment history, income, level of indebtedness, and others. Based on this profile, a loan may be automatically denied. This is a classic case of profiling that results in an automated decision with a significant impact, falling under the provisions of Article 22.

✓ **Algorithms for candidate selection:** Many companies use ATS (Applicant Tracking Systems) and AI-based tools that automatically filter candidates based on keywords, previous experience, or education. When the algorithm automatically rejects a candidate without human review, this constitutes an automated decision. If a model is used to “evaluate” the candidate’s potential, this also involves profiling.

✓ **Targeted advertising:** Platforms such as Facebook and Google use complex profiling algorithms to deliver personalized advertisements based on behavior, interests, and search history. Although these typically do not produce legal effects, in certain cases (for example, behavioral pricing systems or manipulation of elections), they can have a significant impact on the individual and raise ethical and legal concerns.

3.4. Ethical and Legal Challenges

Automated decision-making and profiling create significant risks, including:

Lack of transparency (the so-called “algorithmic black box”)

Discrimination (e.g., based on gender, race, or social status resulting from a trained model)

Unfairness and errors (e.g., unjust denial of a service due to inaccurate data)

Limitation of individual autonomy and choice

The GDPR introduces mechanisms to address these risks, including:

- Obligation to inform (Articles 13–14)
- Right to human intervention and appeal (Article 22, paragraph 3)
- Requirement to carry out a Data Protection Impact Assessment (DPIA) when a given processing activity is likely to result in a high risk.

4. Limitations and rights of data subjects in automated decision-making (Art. 22 GDPR)

The basic principle introduced by Art. 22 states that the data subject has the right not to be subject to a decision based solely on automated processing, including profiling, where such a decision produces legal effects concerning him or her or similarly significantly affects him or her. However, the Regulation provides for several exceptions to this prohibition: where the decision is necessary for entering into, or the performance of, a contract between the data subject and a controller; where authorized by Union or Member State law; or where the data subject has given his or her explicit consent.

In cases where automated decision-making is permissible, the GDPR guarantees the data subject rights of protection, including the right to human intervention, the right to express his or her point of view and the right to contest the decision. Furthermore, the controller is obliged to provide the subject with meaningful information about the logic underlying the processing, as well as the significance and foreseeable consequences of such processing.

4.1. Art. 22(1) GDPR.

The general prohibition reads as follows: “The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.”

This constitutes a general prohibition on decisions that:

- Are entirely automated, i.e. there is no human intervention;
- Have a significant impact on the individual – be it legal effects (e.g. refusal of credit, termination of a contract) or other significant effects (e.g. restriction of access to social services, selection for employment).

This paragraph aims to prevent the depersonalization of decision-making, whereby individuals are subject to algorithmic assessments without the possibility of control, reaction or understanding of the reasons.

4.2. Exceptions to the prohibition (Art. 22, paragraph 2) .

Although a general prohibition applies, Art. 22, §2 introduces three exceptions where automated decisions are permissible, provided that they are accompanied by appropriate safeguards:

a) Necessity for entering into or performing a contract: The decision is permissible if it is necessary for entering into or performing a contract between the subject and the controller (Art. 22(2)(a)). For example: an automated online credit application where a scoring algorithm determines the terms.

Here, “necessity” must be interpreted strictly – not just convenience or efficiency, but a real necessity, without an alternative by human judgment.

b) Explicit consent of the subject: If the subject is explicitly informed and has given freely given, specific, informed and unambiguous consent, the controller may implement automated decisions (Art. 22(2)(c)).

Consent must be:

Separate from other terms (not part of general terms and conditions);

Subject to withdrawal;

Preceded by a clear explanation of the impact of the decision.

c) Legal authorization (legal framework): Where such processing is authorized by Union or Member State law, including for the purpose of preventing fraud, money laundering, compliance with regulatory requirements, etc. In this case, the legal act must provide for appropriate safeguards for the rights and interests of the subjects (Art. 22(2)(b).

4.3. Right to human intervention and appeal (Art. 22(3).

Where an automated decision falls under one of the exceptions, the GDPR obliges the controller to provide safeguards, including the following rights of the subject:

a) Right to human intervention: The subject has the right to request the intervention of a human being to review and assess the automated decision, assess its justification and confirm, amend or revoke it. This makes the process more transparent and reduces the risk of unlawful or unfair results.

b) Right to express his/her point of view: The GDPR recognises the right of the subject to express his/her point of view on the decision, which may be the basis for a re-assessment by the controller.

c) Right to appeal against the decision: The individual has the right to challenge the automated decision by requesting that the decision be reconsidered, amended or revoked by the controller.

These rights are not just a formality – they must be effective, which implies:

- ✓ Existence of a real procedure;
- ✓ Access to a person capable of reviewing the case;
- ✓ Legal possibility of appeal to a supervisory authority or court;

4.4. Obligations for transparency and explainability.

In addition to providing the right to object, the GDPR obliges controllers to ensure transparency at the initial stage of processing:

a) Information about the existence of automated decision-making.

According to Art. 13(2)(f) and Art. 14(2)(g), when personal data are collected, the subject must be informed if:

Automated decision-making will be applied;

Including profiling;

What is the logic of the processing, as well as the significance and expected consequences of it.

b) Disclosure of the logic of the algorithm.

Full disclosure of the program code is not required, but a clear and accessible explanation must be given of:

What data are used;

What criteria influence the result;

What consequences it may have for the individual.

c) Relevance to the right of access (Art. 15).

The subject has the right, upon request, to obtain a copy of the data used in the decision and information about automated decision-making, including profiling, within the framework of the right of access.

4.5. Practical relevance and challenges.

Despite the formal legal framework, in practice many challenges remain:

Algorithmic opacity (so-called black-box AI), where even developers cannot always explain the final decision;

Indirect discrimination, where seemingly neutral data leads to unequal outcomes;

Difficulties in exercising the right to appeal, especially if clear mechanisms are lacking;

Illusion of consent, where individuals are not fully aware of the consequences of automated decisions, despite having "consented".

5. Practical challenges in the context of automated decision-making and data protection

The application of the provisions on automated decision-making poses a number of practical and technological challenges for organisations. On the one hand, the need for transparency and explainability of algorithms contradicts the common "black box" of modern machine learning models. On the other hand, organizations should ensure adequate mechanisms for human intervention that are real, effective and legally binding.

Furthermore, the implementation of a Data Protection Impact Assessment (DPIA) is mandatory in cases where there is a high risk to the rights and freedoms of data subjects, which is often the case with complex automated decisions. The lack of clarity on the scope of "significant impact" and the assessment of "adequacy" of human intervention continue to be a subject of debate in scientific and professional circles.

Although the GDPR establishes clear rules for the protection of personal data in the context of automated decision-making and profiling, its practical application faces a number of significant challenges, especially when it comes to balancing innovation with the protection of data subjects' rights. Here are the main issues and practical solutions that stand out in this regard:

5.1. Balancing innovation and privacy.

With the development of artificial intelligence (AI), machine learning and big data, organizations increasingly rely on automated solutions that are based on algorithms and predictive models to increase efficiency, personalize services or optimize processes. The problem is that these innovations may face the limitations and requirements of the GDPR, such as:

- *Obligation for transparency* – how to provide the necessary information about algorithms without compromising trade secrets or revealing all intellectual property?
- *Obligation for information to data subjects* – how to explain the logic of complex algorithms in a way that is understandable to the average user?

Faced with these challenges, companies must find a compromise between:

- *Innovations* that seek to increase competitiveness, improve products and services and provide a better user experience;
- *Data protection*, which includes the principles of transparency, data subject rights and justification of decisions. Many organizations choose to implement explainable algorithms (e.g., models that are easy for humans to interpret) in an attempt to create verifiable and traceable processes that meet GDPR requirements without sacrificing the effectiveness of their technology solutions.

5.2. How organizations are addressing explainability requirements.

The GDPR places clear requirements on the information and explainability of automated decisions that affect data subjects, but at the same time many companies face difficulties in explaining the complexity of the algorithms used. Even in the case of machine learning, where black box methods are used, organizations must ensure:

Creating explainable algorithms: Many companies are moving towards using explainable machine learning models (e.g. LIME and SHAP), which aim to ensure the understandability of the models and their results by explaining which data features had the greatest impact on the final result.

Transparency of processes: Organizations must ensure clear communication about the ways in which they use automated decisions and what data is collected and processed. They must explain not only what decision was made, but also why it was made, based on which parameters and for what purposes.

Example: In cases of automated credit approval, banks must explain to the customer what factors led to the rejection of credit (for example, poor credit history or high debt-to-income ratio), without revealing details that could violate trade secrets.

Ensuring the right to human intervention: According to Art. 22 of the GDPR, any automated decision-making system has the obligation to provide the possibility of human intervention. This means that data subjects must be able to lodge a complaint or request a review by a human operator.

Conclusion

The GDPR represents a quantum leap in the evolution of European data protection law. Through its clearly defined principles, strong rights for individuals and strict obligations for organizations, the Regulation creates a stable and predictable framework. Automated decision-making and profiling are an inevitable part of today's digital environment, but their use should be carried out within clearly defined legal and ethical boundaries.

The GDPR provides appropriate tools to protect data subjects through the rights of information, objection, access and human intervention. For organisations, this means not only complying with legal requirements, but also building trust through transparency, accountability and responsible use.

Article 22 of the GDPR represents one of the most progressive and important instruments in European law to limit the potential misuse of automated technologies, especially as the GDPR creates a balanced regulatory framework that simultaneously recognizes the benefits of automation and artificial intelligence, but foregrounds the need to protect the fundamental rights and freedoms of individuals.

In the context of dynamically evolving technologies, the challenges of interpreting and implementing the provisions on automated decision-making remain significant. Therefore, efforts to build on good practices, increase expertise and adapt to new technological realities are crucial for the successful implementation of the GDPR for the benefit of society.

Acknowledgments

This article is supported by internal research project RD-08-109/05.02.2025 “Design and build a scalable research platform for Edge AI/HPS analytics”, Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences, Department of Communication and Computer Engineering and Security Technologies.

References:

[1] Article 29 Working Party. (2018). Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679 (WP251rev.01).https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49826.

[2] Boyanov, P., Implementation of TCP SYN flood cyber attack in the computer network and systems. A refereed Journal Scientific and Applied Research, Konstantin Preslavsky University Press, 2019, 17, 36-42, ISSN 1314-6289 (Print), ISSN 2815-4622 (Online), DOI: https://doi.org/10.46687/jsar.v17i1.270.

[3] Boyanov, P., Basic network penetration testing with the network tool Netcat in Linux-based operating systems. A refereed Journal Scientific and Applied Research, Konstantin Preslavsky University Press, Vol. 25, Shumen, 2023, ISSN 1314-6289 (Print), ISSN 2815-4622 (Online), pp. 15-30, DOI: https://doi.org/10.46687/jsar.v25i1.377.

[4] Dimanova, D., Kuzmanov, Z. Development of an Integrated Security and Communication System, International Scientific Referenced Online Journal, issue 63, November 2019, ISSN: 2367-5721, www.sociobrains.com. pp. 83-91.

[5] Dimanova, D., Kuzmanov, Z. Risk Measurement and Assessment. SocioBrains, international scientific online journal, publisher: www.SocioBrains.com, ISSN 2367-5721, pp. 63–69, issue 32, April 2017.

[6] European Data Protection Board (EDPB). (2020). Guidelines 05/2020 on Consent under Regulation 2016/679 (version 1.1).

[7] European Data Protection Board (EDPB) – Guidelines and Opinions.

[8] Goodman, B., & Flaxman, S. (2017). European Union regulations on algorithmic decision-making and the “right to be explained”. AI Magazine, 38(3), 50–57.

[9] Guidelines on Automated Individual Decision-Making and Profiling (WP251 rev.01).

[10] Kuzmanov, Z., Cyberterrorism – definition and forms. SocioBrains, www.sociobrains.com, Published by: Veselina Nikolaeva Ilieva, Bulgaria, issue 76, December 2020, p. 151, ISSN 2367-5721, (online) – (Bulgarian language).

[11] Metodieva, T., "National and Corporate Security," NK with international participation "MATTEX 2018," Shumen University "Bishop Konstantin Preslavski," October 25-27, 2018, Shumen, ISSN: 1314-3921, vol. 2, 2018.

[12] Metodieva, Ts., "Corporate Security and Its Components." Yearbook of Shumen University "Bishop Konstantin Preslavski," pp. 338-341, ISSN 1311-834X, 2020 (Bulgarian language).

[13] Regulation (EU) 2016/679 (GDPR).

[14] Voigt, P., & Von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR): A Practical Guide. Springer International Publishing.

[15] Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why there is no right to be explained to automated decision-making in the General Data Protection Regulation. International Data Protection Law, 7(2), 76–99.