GDPR-Compliant Automated Decision-Making Systems

Leonardo Oliveira Pereira
University of Coimbra, Department of Informatics Engineering, Portugal
uc2020239125@student.uc.pt

***Abstract*—This assignment explores GDPR compliance in automated decision-making systems, examining challenges, strategies, and implications. The study involves reviewing GDPR provisions, analysing case studies, and comparing compliance approaches. Key findings emphasise the need for transparency, fairness, and data protection in GDPR compliance. The research benefits organisations, regulators, and individuals by guiding responsible and ethical ADM processes.**

Keywords—GDPR, ADM, transparency, fairness

I. Introduction

Automated decision-making systems (ADMS) such as predictive analytics, autonomous vehicles, user profiling, automated credit decisioning, and more, have become common in our quickly developing digital age, revolutionizing a variety of societal sectors, including healthcare, banking, education, and beyond [60]. These technologies have boosted productivity, streamlined procedures, and created new opportunities for innovation thanks to their sophisticated algorithms and large data sets [63]. However as technology has advanced, it has also created new moral and legal issues, particularly within the domains of privacy, data protection, and individual rights [60].

The European General Data Protection Regulation (GDPR) [5] superseded the Data Protection Directive (95/46/EC) [4], a crucial piece of legislation that the European Union approved in 2018, lies at the center of these concerns. The GDPR was developed in response to the growing demand for extensive data protection regulations, particularly in conjunction with the recent advances in ADMS. It significantly changes how businesses manage personal data by imposing strict guidelines for accountability, fairness, and transparency.

The convergence of automated decision-making systems with GDPR is a fundamental shift in how we see technology, rather than merely a legal or regulatory issue. It's an awareness that the moral and ethical ramifications of these systems' actions need to be carefully analysed as they become more sophisticated [48]. This assignment takes an in-depth look at this intersection, breaking down its challenges, looking at practical solutions, and highlighting the ethical and legal implications.

It is inconceivable to overestimate the significance of such intersection. Conforming to legal obligations is just one aspect of GDPR compliance within ADM [68]; other goals include promoting a culture of data ethics and ensuring that individuals take care of control over their personal data [62] [35]. It involves developing innovative and efficient systems while simultaneously respecting privacy and human dignity.

In this context, this assignment aims to explain the complexities of GDPR compliance within ADMS. This research seeks to provide a comprehensive understanding of the ethical and legal landscape by examining the key concepts of GDPR, analysing current problems that organisations face, and investigating innovative strategies used to guarantee compliance. It is expected that this investigation will help clarify the way moving forward and point out individuals, organisations, and regulators throughout the direction of ethically and responsibly meant ADMS.

The remainder of the paper is structured as follows: Section II will provide some common ground. Sections III, IV, and V, explore the GDPR principles and examine the role of Data Protection Impact Assessments (DPIAs), identify obstacles in achieving it, and investigate strategies, respectively. Section VI studies legal consequences of GDPR non-compliance and section VII explores how it safeguards individual rights in ADM. Section VIII analyses emerging technologies and finally, conclusions will be presented in section IX.

II. Common ground

Before discussing the GDPR compliance within ADMS, it is provided some background on the key concepts about GDPR and ADM and the rise of ADMS and its applications.

A. *Key Concepts:GDPR and ADM*

Understanding the fundamental ideas that support both the GDPR and ADMS is essential to comprehending the intricate relationship between them.

The world's toughest privacy and security legislation is called the GDPR. Despite being drafted and approved by the EU, it imposes obligations on organisations worldwide, provided that they target or gather data related to individuals inside the EU. The regulation became effective on May 25, 2018. If someone violates the GDPR's security and privacy demands, they could face fines of up to tens of millions of euros [7]. According to the EU, the GDPR was created to "harmonise" data privacy laws among all of its member nations while also giving individuals more rights and protection. The GDPR was also designed to change how businesses and other organisations manage the personal data of people who interact with them [42].

Making decisions automatically, without the need for human intervention, is known as ADM. These decisions may be based on inferred data, digitally generated profiles, or factual data. An online loan award decision and an aptitude test used for hiring that uses pre-programmed algorithms and criteria are two examples of this. Profiling is a common practice in ADM, but it does not have to [33].

B. The Rise of ADM and Its Applications

The exponential growth of data and computational power has been closely related to the rise of ADMS. Processing large amounts of data quickly and accurately has become vital as organisations gather huge amounts of data. The pervasiveness of digital technologies is leading to an increase in ADM [28]. ADM comprises an expanding array of intelligent technologies such as deep learning and blockchains [27]. It was developed to solve challenging problems across sectors to make essential services more personal and help to broaden choices and control for citizens and communities [27].

ADMS have found applications in diverse fields, revolutionizing industries and enhancing efficiency. Some of them include:

- AI-powered systems that can assist with decision-making when the data, parameters, and variables involved are beyond human comprehension [57]. For example, AI can help diagnose diseases, optimize supply chains, recommend products, and detect fraud.
- digitalisation that allows businesses to operate at an atomic level and make millions of decisions each day about a single customer, product, supplier, asset, or transaction [64]. For instance, ADM can help with pricing, marketing, inventory management, and customer service.
- Automation that has the potential to replace middle-skilled workers in any environment where work is predictable and processes remain structured [58]. As an illustration, automation can perform tasks such as manufacturing, food preparation, and retail sales.

The fast development of ADMS resulted in unprecedented conveniences but also brought up some challenges and risks, such as:

- Ethical, moral, and social implications of delegating decisions to machines that may not capture or respond to intangible human factors that go into real-life decision-making [57]. For example, AI may not consider the fairness, accountability, transparency, and explainability of its decisions.
- Human oversight and intervention of ADMS that may require complex and dynamic interactions between humans and machines [64]. For example, humans may need to monitor, evaluate, and override the decisions made by ADMS when necessary.
- Legal and regulatory frameworks that may not be adequate or consistent to address the issues and impacts of ADM on society [27]. For example, ADM may raise questions about the liability, responsibility, and rights of the parties involved in the decision-making process.

By placing these ideas in their proper context, we can better understand how difficult it is to balance technological progress with ethical considerations and the legal obligations.

III. GDPR Compliance Framework

The GDPR provides a strong framework that regulates how organisations handle personal data, especially when it comes to ADM. It is essential to comprehend how it applies to these systems in order to navigate ethical and legal landscape. Regardless of the organisation's location or the location of the data processing, it applies to any entity that handles personal data of individuals in the EU [15].

Since they process personal data to make decisions that have a substantial impact on individuals, ADMS have been regulated under the GDPR. The GDPR's Article 22 addresses ADM particularly, emphasising the right to human intervention and transparency in the context of profiling.

A. Principles of GDPR

GDPR establishes precise guidelines for ADM to guarantee the protection of people's rights and keep organisations accountable for how they handle personal data. Some of the GDPR principles that are relevant to ADM are [15] [17]:

- **Transparency:** Organisations must provide meaningful information to individuals about the ADM process, including the logic behind the decision, and the implications for the individual. Individuals have the right to access, rectify, and erase their personal data, as well as to object to or restrict the processing of their data.
- **Fairness:** Organisations must ensure that the ADM process does not discriminate against or harm individuals on the basis of their personal data, such as their race, gender, age, or disability. Individuals have the right not to be subject to a decision based solely on automated processing, unless it is necessary for a contract, authorised by law, or based on their explicit consent.
- **Accountability:** Organisations must be able to demonstrate that they comply with the GDPR principles and requirements when using ADM. They must also implement appropriate technical and organisational measures to ensure the security, accuracy, and quality of the personal data and the ADM process.

B. Role of Data Protection Impact Assessments (DPIAs)

One of the measures that organisations may need to take when using ADM is to conduct a Data Protection Impact Assessment (DPIA). A DPIA is a procedure that assists institutions in identifying and minimising the risks to data protection associated with projects or processes that involve personal data [32]. When using ADM that has significant or legal implications for individuals, or when processing personal data in any other way that represent a high risk to their rights and freedoms, a DPIA is indispensable. It should include these steps [31]:

- Step 1: identify the need for a DPIA
- Step 2: describe the processing

- Step 3: consider consultation
- Step 4: assess necessity and proportionality
- Step 5: identify and assess risks
- Step 6: identify measures to mitigate the risks
- Step 7: sign off and record outcomes

In order to identify and mitigate risks associated with the deployment of ADMS, organisations must conduct DPIAs and ensure that the processing is compliant with GDPR requirements. In the context of ADM, understanding and putting these GDPR regulations into practice not only guarantees legal compliance but also establishes a framework for ethical data practices. It emphasises the value of transparency, fairness, and accountability in building trust between individuals and organisations in a period where decisions based on data are influencing various aspects of our lives.

IV. Challenges in Compliance

Businesses all over the world have been greatly impacted, changing how they handle personal data and emphasising data security and privacy more than before [49].

Handling GDPR compliance in ADMS is a complex task with many moving parts, each of which presents a different challenge to following the regulations and ethics. The challenges for GDPR in Article 22 include the rights of individuals not to be subject to ADM without explicit consent, the requirement for organisations to provide an explanation of how decisions are reached, and the need for appropriate mathematics and statistical procedures. Because they call for a privacy by design approach (Art. 25), the completion of a Data Protection Impact Assessment (Art. 35), and ethical approval, these challenges are especially relevant to research projects involving computational intelligence. Although the GDPR's research legal framework tackles certain obstacles, it still leaves open questions about the processing of special categories of data and the legal basis for processing them. As a result, it is challenging for EU researchers to make progress toward AI that is trustworthy.

Understanding these challenges is decisive for organisations seeking to deploy ADMS responsibly.

A. *Algorithmic Bias*

One of the main risks associated with ADM is the possibility of discrimination [38]. Algorithms are designed for people, so, like humans themselves, they can carry inherent (or not inherent) biases that can provoke discriminatory outcomes regarding data subjects' characteristics, such as, their ethnic origin, sexual orientation, economic situation, gender, among others [38].

High-quality decision-making is dependent on data quality, as it is difficult to make well-informed decisions in the absence of reliable data [36]. Biases inherent in training data can lead to unfair outcomes, infringing upon the GDPR principles of fairness and non-discrimination. Identifying and rectifying these biases in ADM processes is a complex task.

Some examples of algorithmic bias in ADM which violates the GDPR article 22 are [15]:

- **Credit scoring:** Some credit scoring systems may use personal data, such as age, gender, or ethnicity, to assess the creditworthiness of applicants. This may result in biased decisions that deny credit to certain groups or individuals based on their protected characteristics, rather than their actual financial situation. This could be against both Article 22 and Article 9, which forbids processing certain types of personal data unless there is a legitimate reason and appropriate protections in place.
- **Recruitment:** Certain hiring systems may rank and filter job applicants using automated processing, such as personality assessments or resume screening. This could result in prejudiced assessments that favor or disfavor specific groups or individuals based on personal information about them, such as their knowledge base, education, or appearance. This may violate Article 22, as well as Article 21, which gives data subjects the right to object to the processing of their personal data for direct marketing or profiling purposes.
- **Healthcare:** Some healthcare systems may use automated processing, such as diagnosis or treatment recommendations, to provide medical services to patients. This might result in biased decisions that impact specific groups' or individuals' access to and quality of healthcare depending on their personal information, such as location, lifestyle, or health. Both Article 22 and Article 9, which demand a legitimate basis and appropriate safeguards for the processing of certain categories of personal data, like health data, may be broken by this.

B. *Transparency*

As already mentioned, one of the most important GDPR requirements is to provide clear and transparent information about how personal data is processed. Individuals need to be provided with a meaningful explanation of the logic behind the AI system, as well as the possible consequences of the processing [29].

The "black box" problem, which refers to the inherent opacity of many ADM algorithms, is one of the main obstacles. It can be difficult to explain how decisions are made in a way that is both clear and understandable due to the complexity of these algorithms. Transparency is required by the GDPR as a basic principle, and organisations must communicate processing information to data subjects in a comprehensible, accessible, and concise manner. It's still very difficult to strike a balance between the complexity of sophisticated algorithms and the requirement for transparency.

Using the previously mentioned examples, here are the scenarios where we can identify the challenges of the "black box" problem complying with the article 22 of the GDPR:

- **Credit Scoring:** A credit scoring company uses a deep neural network to assess the creditworthiness of loan applicants. The company does not disclose how the network was trained or what features it uses to make its decisions. A customer is denied a loan and wants to know why, but the company cannot explain the logic behind

the network's output. This violates the customer's right to contest the decision and to obtain human intervention, as stipulated by article 22 of the GDPR [37].

- **Recruitment:** A recruitment company uses a natural language processing system to analyse the resumes and cover letters of job applicants. The system assigns a score to each applicant based on their qualifications, skills, and personality. The company does not reveal how the system works or what criteria it uses to evaluate the applicants. An applicant is rejected and wants to know the reasons behind the decision, but the company cannot provide any feedback or justification.This violates the applicant's right to obtain an explanation and to challenge the decision, as required by article 22 of the GDPR [53].
- **Healthcare:** A healthcare provider uses a support vector machine to diagnose patients with skin cancer based on images of their skin lesions. The provider does not reveal the details of the machine learning model or the data it was trained on. A patient is diagnosed with melanoma and wants to know how confident the model is and what factors influenced its decision. The provider cannot provide any explanation or justification for the model's output, as the support vector machine is a black box that only outputs a binary label (cancer or no cancer). This undermines the patient's trust and confidence in the diagnosis, as well as the provider's accountability and responsibility for the outcome [41].

C. *Data Minimisation*

The GDPR strongly promotes the idea of data minimisation, arguing that you only should collect and process personal data that is absolutely necessary to fulfil your purpose [18]. ADMS often rely on vast datasets for optimal performance, creating a tension between the utility of extensive data and the imperative to minimise data processing for privacy reasons.

However, implementing data minimisation in ADMS can be challenging for several reasons:

1) **Determining the minimal amount of data:** It can often be difficult to determine the minimal amount of data required, especially in complex machine learning models such as deep neural networks [52].
2) **Lack of transparency:** Often referred to as "black box" models, ADMS make it challenging to identify precisely which data influenced the decision. This lack of transparency can lead to breaches of lawful grounds for processing, such as obtaining consent which is invalid because there is not enough transparency about the ADM [56].
3) **Violation of Article 22 of the GDPR:** Under Article 22 of the GDPR, data subjects have the right not to be subject to a decision based solely on automated processing, such as profiling, or any activity, that, "produces legal effect concerning him or her or similarly significantly affects him or her." [56].

Here are some examples where the vast amount of data collected from the ADMS could lead a violation of the article 22 from GDPR:

- **Education:** ADMS are increasingly being used in the education sector for purposes such as grading, personalised learning, and predicting student performance. However, these systems may use a wide range of personal data about students, including their age, gender, ethnicity, socioeconomic status, and even behavioral data. This could potentially lead to biased decisions that unfairly affect certain groups of students.
- **Insurance:** ADMS in the insurance industry might use personal data such as age, gender, health status, and lifestyle habits to assess risk and determine insurance premiums. This could potentially lead to biased decisions that unfairly affect certain groups of individuals based on their protected characteristics.
- **Retail:** In the retail sector, ADMS might use personal data such as shopping habits, location, and socioeconomic status to personalise marketing and product recommendations. This could potentially lead to biased decisions that unfairly target or exclude certain groups of customers.

In all these examples, it's crucial to ensure that any personal data used is properly safeguarded to protect individuals' privacy. Regular reviews and updates should also be conducted to ensure ongoing compliance with GDPR principles.

V. Compliance Strategies

To comply with GDPR regulations in ADM, organisations must ensure that their decision-making processes are transparent, provide meaningful information to data subjects, obtain explicit consent from data subjects, implement measures to prevent bias and discrimination, and conduct DPIAs [32].

A key component of compliance is explicit permission, which mandates that businesses notify people of the specific purposes of the collection, processing, and use of their personal data in ADM (Art. 4; Art. 6). In addition, data subjects need to be informed of their ability to object to these kinds of activities and provided with the necessary information in order to properly exercise that right (Art. 21).

Mitigating bias and discrimination within ADM processes is paramount for GDPR adherence. Organisations must ensure that their systems do not unfairly discriminate based on protected characteristics such as race, gender, age, religion, or disability (Recital 71). Regular reviews of decision-making processes are essential, enabling the identification and rectification of potential biases to maintain fairness and equity.

Conducting DPIAs emerges as a non-negotiable aspect of GDPR compliance in ADM. These assessments serve as a proactive measure to identify and minimise risks associated with the processing of personal data. Organisations are mandated to conduct DPIAs before implementing ADM processes that pose high risks to the rights and freedoms of data subjects (Art. 35).

In addition to meeting the GDPR requirements, here are some practices recommendations, each of them followed by an

intuitive example, that organisations should consider to help ensure compliance with GDPR in ADM:

- **Proactive Integration of Privacy by Design and Default:** Proactively integrating privacy considerations into ADMS' default settings and design is a fundamental component of GDPR compliance efforts (Art. 25). Privacy by Design holds that organisations need to consider privacy at the initial design stages and throughout the complete development process of new products, processes, or services that involve processing personal data [47]. Privacy by Default means that when a system or service includes choices for the individual on how much personal data he/she shares with others, the default settings should be the most privacy-friendly ones [47]. By incorporating privacy measures into systems from the very beginning, organisations reduce the chance of non-compliance and increase user trust. This strategy aligns with the GDPR's emphasis on data protection as an integral part of the technology life cycle.
  Example: A leading technology firm incorporates privacy features directly into the algorithmic design of its decision-making system, ensuring that data protection measures are seamlessly integrated into the core functionality.
- **Comprehensive DPIAs:** DPIAs play an important role in understanding and mitigating the risks associated with ADM processes (Art. 35). Organisations undertake thorough assessments to identify and address potential privacy and compliance issues. This strategy not only ensures compliance with GDPR but also fosters a proactive risk management approach, enhancing overall system robustness.
  Example: A financial institution conducts a DPIA before implementing an automated credit scoring system. This assessment identifies potential biases and ensures that the system adheres to GDPR principles, fostering transparency and fairness.
- **Transparent Data Processing Policies and Practices:** One of the main components of GDPR compliance is transparency. Organisations must ensure that their ADM processes are fair, transparent, and accountable (Art. 5). This means providing meaningful information to individuals about the ADM process, including the logic behind the decision, and the implications for the individual [32]. This includes checking data sets for bias, regularly reviewing the accuracy and relevance of decisions, deploying systems that audit algorithms, and using appropriate procedures and measures to prevent errors, inaccuracies, or discrimination [55]. Clear communication builds trust and empowers individuals to make informed choices regarding their data.
  Example: An e-commerce platform provides users with detailed information on how its recommendation engine operates, what data is used, and how users can customize their privacy settings, aligning with GDPR transparency requirements.
- **Regular Audits and Continuous Monitoring:** Compliance is a continuous commitment rather than a one-time occurrence. Organisations should implement regular audits and continuous monitoring mechanisms to ensure that ADMS adhere to GDPR principles (Art. 32). This strategy involves periodic reviews of data processing activities, algorithmic outputs, and system updates, fostering a culture of accountability and adaptability. It is crucial to designate a DPO (Data Protection Officer) (Art.37).
  Example: A healthcare provider conducts regular audits of its diagnostic decision support system, verifying that the system's outputs align with medical standards and comply with GDPR requirements for sensitive health data.
- **Collaboration with Data Protection Authorities:** Engaging in open and collaborative relationships with data protection authorities is an emerging strategy for organisations navigating GDPR compliance. Proactively seeking guidance and feedback from regulatory bodies demonstrates a commitment to compliance and facilitates a shared understanding of evolving regulatory expectations.
  Example: A telecommunications company collaborates with the national data protection authority to ensure that its automated customer service system aligns with GDPR requirements, fostering a cooperative approach to compliance.
- **Incorporating the Right to Challenge and Request Human Intervention:** A critical aspect of GDPR compliance strategies involves acknowledging and respecting the rights conferred upon data subjects by Article 22. This article grants data subjects the right to object and express their point of view regarding any ADM, and the right to demand human intervention [65]. Establishing procedures that let data subjects contest automated judgments and ask for human intervention when needed is crucial for organisations. In line with the GDPR's commitment to safeguarding data subjects' rights and freedoms, this proactive approach guarantees that people maintain influence over choices that impact them.
  Example: An online recruitment platform implements a feature that enables job applicants to challenge automated hiring decisions. In response to challenges, the system initiates a human review process to ensure fairness and transparency.
- **Employee Training and Awareness Programs:** Human factors play a crucial role in GDPR compliance. Organisations invest in comprehensive training and awareness programs to educate employees about the importance of data protection, ethical decision-making, and their role in ensuring compliance. Well-informed employees contribute to a culture of responsible data handling.
  Example: An educational technology company conducts regular workshops for its development team, emphasising

the ethical considerations of algorithm design and the implications for GDPR compliance.

To help companies comply with GDPR, the European Data Protection Board has published guidelines on ADM and profiling [28]. These guidelines provide practical examples of how organisations can implement the best practices for GDPR compliance in ADM. Additionally, a company called "DPOrganizer" provides a GDPR compliance software that helps organisations manage their data processing activities [2]. The software includes features for transparency, consent management, bias and discrimination prevention, DPIA, and human review.

As organisations embrace these strategies, they not only mitigate legal risks but also contribute to a more ethical and responsible landscape for ADM, aligning with the overarching goals of GDPR.

A. PROS Holdings, Inc. Case Study

PROS Holdings, Inc. (NYSE: PRO) is a company that provides AI-powered SaaS (Software as a Service) solutions. Their mission is to help people and companies outperform by enabling smarter selling in the digital economy. They've developed predictive and prescriptive guidance over decades of testing in complex, real-world business cases [6].

The Information Security Compliance team at PROS, Inc needed to get away from the time-consuming manual tracking of spreadsheets saved on SharePoint in order to effectively manage audits and tackle GDPR compliance [24].

After reviewing several compliance software platforms, the Information Security Compliance team realized Onspring provided the most robust and practical approach to managing GDPR compliance [24]. Here are some of the key steps they took [24]:

- **Moving away from manual tracking:** The Information Security Compliance team at PROS, Inc needed to move away from time-consuming manual tracking of spreadsheets saved on SharePoint in order to effectively manage audits and tackle GDPR compliance.
- **Implementing new procedures, audits, and reporting:** New considerations from GDPR regulation required the team to start planning for implementation of new procedures, audits, and reporting to document not only their own compliance but all third-party processors.
- **Updating third-party contracts:** Contract updates were required to reflect adherence to GDPR regulations. Risk assessments had to be conducted to evaluate each vendor's security framework. Any third-party processor not in compliance would violate PROS GDPR compliance.
- **Creating response plans:** New data protection plans needed to be created and maintained. Incident response plans for GDPR data requests needed to be created and tested. Periodic risk assessments specific to those plans needed scheduling and deployment.

This case study demonstrates how PROS, Inc. managed to effectively tackle GDPR compliance by adopting a robust compliance software platform and implementing a range of new procedures and plans. It is important to note that the specifics of GDPR compliance can vary depending on the company's operations and the nature of the data they handle.

B. The Swedish National Board of Student Aid (CSN) Case Study

Before talking about this case study, it is important to mention that it refers to times before the GDPR came into force but nevertheless presents good practices that would make it possible to comply with its regulations

This study highlights that the rise of e-government has led to an increase in ADM, forming part of a trend towards "smart" and self-regulating systems [70]. This shift necessitates the introduction of new relationships and practices, challenging the traditional division of responsibilities in public administration.

The Swedish National Board of Student Aid (known as the CSN) manages the payment of financial aid to students for their living costs. Despite concerns in the 1970s about potential job losses and decision transparency, Sweden has continued to embrace digitalisation and the CSN has evolved with the introduction of numerous e-services and automation initiatives.

The study focuses on the CSN's "In" unit, which handles loan repayments and utilizes automated systems for decision-making. Several approaches and strategies have been observed in how CSN integrates ADM while addressing the challenges and ethical considerations associated with this technology [70]:

- **Strict Adherence to Legislation:** CSN's ADM system strictly follows legislation, acting as a mediator of the law. The system is viewed as a key actor within a network, and professional officers support its decisions.
- **Balancing Ethics of Care and Ethics of Justice:** Decisions are largely rule-based and justice-oriented, officers may apply a degree of ethics of care in more complex situations, such as when clients request lower reimbursement amounts due to mitigating circumstances.
- **Client Guidance and Support:** When clients interact with CSN, officers play a guiding role, preparing clients for automated decisions. The emphasis is on demonstrating the correctness of the system's decisions and explaining the rationale behind them.
- **Two Strategies for Client Interaction:** CSN officers adopt two main strategies when clients challenge decisions:
  - In Strategy A, officers defend the system and legislation, emphasising the correctness of automated decisions.
  - In Strategy B, officers form an alliance with the client against the system, translating client demands into the system to potentially influence a more favorable outcome.
- **Legitimacy through Legislation and Transparency:**The automated system is considered a "hidden bureaucrat," making decisions based on justice, rule of law, efficiency, and equal treatment for clients.

- **Flexibility in Decision-Making:** Professional officers may draw on personal experience, collegian knowledge, and arguments based on an ethic of care to make nuanced decisions.

In summary, CSN has carefully incorporated ADM into its operations by combining rigorous legal compliance, a fair balance between justice and care ethics, individual client guidance, and flexibility in decision-making as needed. The overall goal is to increase systemic confidence while ensuring transparency and accountability in the provision of financial assistance services to students.

VI. Legal and Ethical Implications

The convergence of GDPR and ADMS precipitates a complex web of legal and ethical considerations. This part explores the nuanced environment, looking at the consequences of not complying to GDPR and clarifying the complex relationship between legal and ethical implications.

A. Consequences of GDPR non-compliance

There is no legal consequence resulting from the wording of the Article 22 [19]. However, non-compliance with the GDPR can lead to serious legal consequences. Here are some potential outcomes [1]:

1) **Data breaches and theft of sensitive information:** Not complying with the GDPR implies that you are unlawfully processing personal data of the persons concerned and or not taking the required safety measures.
2) **Complaints by customers, clients and employees:** Citizens are becoming more aware of their privacy, of the importance of data protection, and of the obligations of businesses with regards to data protection.
3) **Administrative audits and administrative fines:** The data protection authorities may start an audit, triggered by a complaint or on their own initiative, when they notice that some of your publicly available information or communications appears to be non-compliant and, if proven, this may result in administrative GDPR fines, which may in theory amount up to 20 million euros (or 4% of the yearly worldwide turnover, if that amount is higher).
4) **Local criminal fines and charges under national law:** Depending on the countries in which you are active, local laws may impose criminal prosecution and fines in case of non-compliance.
5) **Ineligibility to participate in public tenders or work for clients or customers who must be GDPR compliant themselves:** When you provide services to public authorities or to customers or clients in regulated sectors, they will often impose on their suppliers to be GDPR compliant.

In addition to the financial costs, non-compliance damages the organisation's reputation and reduces trust. With increasing public awareness of data privacy issues, individuals are more inclined to scrutinize how organisations handle their data. Consequently, legal consequences extend beyond monetary fines, impacting an organisation's standing in the market and potentially leading to long-term financial repercussions.

B. Caixabank's client profiling Case Study

This case study discusses two decisions by the Spanish Data Protection Authority (AEPD) related to Caixabank's client profiling practices [39].

In January 2021, the AEPD rendered a decision against Caixabank, a major financial institution, regarding its client profiling practices. The AEPD's investigation centered on the application of Article 22(1) of the GDPR, which pertains to ADM (ADM) [15]. Despite the use of customer consent and provisions for human intervention, the AEPD determined that Caixabank's client profiling did not meet the criteria for ADM, as individual decisions were ultimately made by human employees exercising their judgment.

However, the AEPD found that Caixabank fell short on transparency obligations stipulated in Articles 13 and 14 of the GDPR [8] [11]. The Authority invoked Recital 60 of the GDPR, asserting that Caixabank failed to adequately inform data subjects about the types of profiles it intended to create, their specific uses, and the potential consequences for individuals [20]. Additionally, data subjects were not adequately informed about their right to object.

Regarding consent, the AEPD concluded that the obtained consent for client profiling was not valid. The consent lacked the necessary level of informativeness, freedom, and specificity. It was bundled with contractual terms, and data subjects were not sufficiently apprised of the details of the processing activities.

Consequently, the AEPD imposed a significant administrative fine totaling 6,000,000 EUR on Caixabank, highlighting the severity of the transparency breach and the invalidity of the obtained consent. The fine was grounded in the GDPR's principles, emphasising the importance of transparency and lawful grounds for processing personal data.

In a separate case later that year, Caixabank faced another substantial fine of 3 million EUR from the AEPD. This penalty was related to the inadequacy of informed consent for profiling prospects and customers, particularly in the contexts of loan default risk analysis and personalised promotional activities.

The AEPD, in its findings, underscored that the information provided to data subjects was generic and failed to allow them to understand the intricacies of the processing, such as the level of detail in the profiles and their consequential impact. Moreover, data subjects were not afforded the opportunity to separately consent to each profiling purpose, a requirement specified in Article 4(11) of the GDPR [16].

In summary, the Caixabank case study serves as a noteworthy example of the regulatory emphasis on transparency, informed consent, and compliance with GDPR principles in the realm of client profiling. The AEPD's decisions underscore the necessity for organisations to effectively communicate with data subjects, providing clear and detailed information about profiling activities and obtaining valid consent for processing personal data.

C. *Klarna Bank AB Case Study*

This case study discusses a regulatory action taken by the Swedish Data Protection Authority (IMY) against Klarna Bank AB, a financial institution [39].

On March 28, 2022, the IMY imposed a fine of 7,500,000 SEK (approximately 750,000 EUR) on Klarna Bank AB for multiple violations of transparency requirements under the GDPR. The regulator found that, between March and June 2020, Klarna failed to provide meaningful information about the rationale, meaning, and foreseeable consequences of ADM it conducted to assess credit applications and detect potential fraud or money laundering.

The IMY highlighted that Klarna's data protection notice merely mentioned the use of certain types of information (such as contact, identification, and financial information) in connection with automated decisions. However, it did not sufficiently explain to customers the circumstances that could lead to a negative credit decision. The IMY argued that the GDPR requires disclosure of the categories of data crucial to an internal scoring model and the potential circumstances leading to a refusal decision. Since Klarna's notice lacked this information, the IMY determined that the controller violated Articles 13(2)(f) and 14(2)(g) of the GDPR [8] [11].

In essence, the case underscores the significance of transparent communication in ADM processes, with a particular emphasis on informing individuals about the key factors and categories of data influencing decisions that could significantly impact them, such as credit-related determinations. The enforcement action by the IMY highlights the regulatory commitment to upholding GDPR principles and ensuring that organisations fulfill their obligations to safeguard individuals' privacy rights in the age of ADM.

D. *Relationship between legal and ethical implications*

Although the legal consequences are a deterrent, ethical considerations introduce a moral imperative for organisations to go beyond mere compliance. Organisations are urged to move beyond the letter of the law and embrace the spirit of ethical data processing.

The GDPR sets out legal obligations for organisations that process personal data. These include principles such as lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, confidentiality, and accountability [30].

On the other hand, ethical responsibilities under GDPR might include going beyond what is legally required and striving to respect the privacy of individuals, being transparent about how their data is used, and taking steps to protect their data [67].

The main difference between legal compliance and ethical responsibility is that legal compliance is about obeying the law, while ethical responsibility is about doing what is right, sometimes even regardless of the law [67]. In other words, compliance is following the law while ethics is doing what is right, sometimes even regardless of the law.

The GDPR itself reflects ethical principles by emphasising the rights and dignity of individuals. It empowers individuals with rights such as the right to access, rectify, and object to automated decisions made about them (Art. 15; Art. 16; Art. 22). These rights go beyond legal compliance, embodying ethical ideals of respect for individual autonomy and control over personal data.

The interplay between legal obligations and ethical responsibilities creates a dynamic landscape that organisations must navigate. Achieving GDPR compliance becomes not merely a box-ticking exercise but a commitment to ethical behavior, recognizing the profound impact of ADM on individuals and society at large.

In conclusion, the legal and ethical implications of GDPR compliance in ADMS underscore the need for organisations to move beyond regulatory adherence. While legal consequences provide a framework for compliance, ethical responsibilities guide organisations in creating systems that not only meet legal standards but also contribute positively to society. Striking this delicate balance is crucial in fostering a culture of responsible and ethical ADM. As organisations navigate this complex landscape, the synergy between legal obligations and ethical considerations becomes the cornerstone of building trust, safeguarding individual rights, and embracing a future where automated systems align harmoniously with human values.

VII. Impact on Individuals

With the introduction of ADMS under the GDPR, people's lives are profoundly affected, and the dynamics of privacy, autonomy, and decision-making are shifted. This section examines the many ways the GDPR protects people's rights when it comes to ADM, addressing issues and emphasising the critical role that ethical considerations play.

A. *Rights Safeguarded by GDPR:*

GDPR provides several rights to individuals regarding their personal data [21]. Here are the key rights:

1) **Right to Information [8] [11]:** Under Article 13 and 14 of the GDPR, individuals have the right to be informed about the collection and use of their personal data. This includes information about the existence of ADM, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
2) **Right to Access [12]:** Individuals have the right to access their personal data. This means they can request to view and obtain copies of their personal data that an organisation is processing. This right helps individuals understand why and how the organisation is using their data, and to ensure it's being used lawfully.
3) **Right to Rectify [13]:** The GDPR grants individuals the right to rectify inaccurate personal data or have it fully completed if the information is not complete. They can request rectification in writing or verbally and the

company has one calendar month to respond to them formally.

4) **Right to Object to Automated Decisions [15]:** Article 22 of the GDPR provides individuals with the right to object to decisions being made with their data solely based on ADM or profiling. This means individuals should not be subject to a decision that is based solely on automated processing (such as algorithms) and that is legally binding or which significantly affects them. Exceptions are allowed under certain circumstances, such as when the decision is necessary for the entry into or performance of a contract, or based on the individual's explicit consent.
5) **Right to Erasure (Right to be Forgotten) [10]:** Under Article 17 of the GDPR, individuals have the right to have their personal data erased. This right is not absolute and only applies in certain circumstances.
6) **Right to Restrict Processing [9]:** Closely linked to GDPR Article 16 (the right to rectification) and GDPR Article 21 (the right to object), individuals have the right to ask for the restriction or suppression of their personal data. This is not an absolute right and only applies in certain circumstances.
7) **Right to Data Portability [14]:** The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It means they can copy, transfer or move personal data from one online environment to another, safely and securely. It only applies to data an individual has previously provided to a controller.

B. Concerns related to individual autonomy and decision-making:

GDPR has provisions to protect individual autonomy and decision-making, particularly in the context of ADMS. However, there are several concerns related to these areas [40]:

1) **Lack of Transparency:** ADM processes, particularly those involving complex algorithms or machine learning, can be opaque and difficult for individuals to understand. This lack of transparency can make it challenging for individuals to exercise their rights under the GDPR, such as the right to access, rectify, and object to automated decisions.
2) **Potential for Bias and Discrimination:** If the data used to train the algorithms contains biased information, the decisions made by these algorithms could also be biased. This could lead to unfair outcomes, such as discrimination in hiring, lending, or other areas.
3) **Influence on Individual Autonomy:** Automated decisions can significantly influence individuals' circumstances, behavior, or choices1. For example, an algorithm might determine whether someone is eligible for a loan, what kind of news they see online, or even their treatment plan for a medical condition. This can raise concerns about individual autonomy and the ability of individuals to control their own lives.
4) **Risk of Errors:** ADMS can make mistakes, and it can be challenging for individuals to correct these errors if they don't have a clear understanding of the decision-making process. For example, if an algorithm incorrectly determines that someone is a poor credit risk, that person might have difficulty getting a loan, even if they are actually a good credit risk.
5) **Inadequate Consent:** There are cases where consent to partake in an ADM system wasn't sufficient, if the data subject wasn't "adequately informed about the logic behind it" [56]. This raises concerns about the validity of consent in the context of ADM.

C. SyRI Algorithm Case Study [39]

In February 2020, the District Court of The Hague issued a landmark ruling on the Dutch government's System Risk Indication (SyRI) algorithm. SyRI, designed for fraud detection, targeted neighborhoods with minority or low-income populations in the Netherlands. The court determined that while SyRI itself was not aimed at legal effects, the risk reports it generated significantly impacted individuals' private lives, violating Article 8 of the European Convention on Human Rights (right to respect for private and family life) [23].

The court cited concerns about SyRI's lack of transparency and left open the question of whether it violated the GDPR regarding automated individual decision-making and potential exceptions to its prohibition.

Subsequently, the Dutch Data Protection Authority (AP) imposed a €2,750,000 fine on the Dutch Tax and Customs Administration for processing dual nationality status in the SyRI system. The AP deemed this processing discriminatory and unlawful under Article 6(1) GDPR [26], as it was not necessary for the public interest task and breached principles of lawfulness and transparency under Article 5(1)(a) GDPR [22]. The AP emphasised that processing only Dutch nationality would have sufficed, and the discriminatory nature of the processing violated the fairness principle under Article 5 [22]. Notably, no findings were made under Article 22 GDPR in this case [15].

To sum up, GDPR has a significant effect on people when it comes to ADM. It creates a strong framework that protects individual rights and guarantees accountability, fairness, and transparency. The GDPR maintains a careful balance between protecting fundamental rights and advancing technology by giving individuals control over their personal data. By doing this, it not only solves present issues but also establishes the framework for morally sound and accountable ADMS, enabling people in the constantly shifting digital age.

VIII. Future Trends and Developments

Advances in technology and societal changes are expected to bring about significant changes in the field of ADM in the future. This section explores new innovations and trends that will probably influence how ADMS comply with GDPR.

A. *Evolving Technologies*

The future promises an array of cutting-edge technologies that will impact the compliance landscape. Artificial Intelligence (AI) and machine learning, already integral to ADM, are expected to become more sophisticated. Explainable AI (XAI) and federated learning are emerging as solutions to address the "black box" nature of some algorithms, ensuring transparency and interpretability.

- **Explainable AI (XAI) [44]:** Form of artificial intelligence that provides insights into how it makes decisions. It plays a crucial role in regulatory compliance under the European Union's Artificial Intelligence Act (EU AIA). The EU AIA is a legislative effort that aims to ensure AI technologies are used ethically, responsibly, and in a manner that aligns with fundamental rights and societal values. XAI simplifies regulatory compliance by making decision-making more transparent [54]. However, implementing XAI for EU AI Act compliance can present challenges, including the trade-off between interpretability and model complexity, and the need for skilled machine learning engineers, data scientists, and AI solution architects.
- **Federated Learning [43] [50] [69]:** New approach to machine learning where an algorithm is trained on local nodes or devices. It enables devices to learn collaboratively while keeping the data locally. This technology is particularly useful in highly-regulated domains like finance, where regulators prescribe high levels of transparency, assuring the traceability of decisions for third parties. Federated learning can help us withhold privacy, improve security, and comply with privacy regulations. However, it also presents challenges related to the dynamic, distributed, heterogeneous, and collaborative nature of client devices.

Also, there are now more options for protecting and handling personal data thanks to the emergence of decentralized technologies like blockchain. These technologies are in line with GDPR principles since they have the ability to improve privacy and data security through decentralization of control.

- **Blockchain [46] [66]:** Technology that can play a significant role in data protection and compliance. Blockchain applications present a conundrum for many existing data protection laws, which assume a central and identifiable entity that is responsible for complying with the law. On one hand, certain features of blockchain technology, such as encryption and anonymisation, seem to promise better security. On the other hand, certain features such as the immutability of data on the blockchain seem incompatible with requirements relating to correction and deletion. A platform that places decision power on access to personal sensitive data in the hands of the individual that data is about, and ensures full transparency on what that data is used for, by whom, when, and under what specific consent is referred to as "Blockchain for Sensitive Data", or "B4S".

Having said that, XAI, Federated Learning, and Blockchain are powerful technologies that can help organisations navigate the complex landscape of data protection and compliance. However, they also present unique challenges that need to be carefully managed.

B. *Ethical AI Frameworks*

With increasing public awareness and scrutiny, there is a growing emphasis on integrating ethical considerations into AI and ADM. Future developments may witness the establishment of standardized ethical frameworks that guide the development and deployment of these systems. These frameworks should address key ethical considerations such as fairness, accountability, transparency, and privacy.

Moreover, these ethical frameworks should be dynamic and adaptable, evolving with technological advancements and societal changes. They should promote a culture of ethical consciousness and responsibility among AI developers and users.

Finally, it's crucial that these frameworks are not just theoretical but are practically implementable. They should provide clear guidelines and tools to operate ethics in AI, from the design stage to deployment and monitoring [3].

In this way, these frameworks would not only ensure compliance with GDPR principles but also provide a broader ethical foundation for responsible innovation.

C. *Enhanced Human-AI Collaboration*

As AI systems become more prevalent, the future is likely to witness a shift toward enhanced collaboration between humans and machines [34]. This concept, often referred to as 'Augmented Intelligence', emphasises the supportive role of AI in enhancing human decision-making.

Striking the right balance between human oversight and AI autonomy is indeed crucial. While AI can process vast amounts of data and identify patterns far beyond human capabilities, humans bring unique strengths to the table, such as intuition, creativity, and the ability to understand complex social dynamics.

Furthermore, human oversight is essential to ensure that AI systems operate in a manner that aligns with our ethical values and legal norms, including GDPR principles. This includes ensuring transparency in AI decision-making, respecting user privacy, and maintaining fairness in outcomes.

D. *Increased Emphasis on Data Minimisation and Purpose Limitation*

Future trends may see a heightened focus on data minimisation and purpose limitation. These principles, which are core tenets of the GDPR, state that personal data should be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed" [59].

Data minimisation refers to the practice of limiting the collection of personal information to what is directly relevant and necessary to accomplish a specific purpose [25].

Purpose limitation, on the other hand, requires that personal data be collected for specified, explicit, and legitimate

purposes, and not be further processed in a manner that is incompatible with those purposes [51].

There is a growing body of research exploring how these principles can be meaningfully implemented in data-driven algorithmic systems, including personalisation, profiling, and decision-making systems [51].

In the future, we can expect to see advanced data anonymisation techniques and privacy-preserving technologies becoming more commonplace, as organisations strive to align their data practices with these principles and mitigate privacy concerns associated with extensive data collection.

E. Accountability through Auditing and Certification

To ensure ongoing compliance, future developments may include the establishment of auditing and certification mechanisms specifically tailored to ADMS.

In the context of ADMS, ethics-based auditing (EBA) is considered a potential governance mechanism. EBA is defined as a structured process where an entity's present or past behavior is assessed for consistency with relevant principles or norms [61]. This approach can contribute to good governance by promoting procedural regularity and transparency.

However, the implementation of EBA faces several challenges, including conceptual, technical, social, economic, organizational, and institutional constraints. Despite these challenges, EBA is seen as an integral component of multifaceted approaches to managing the ethical risks posed by ADMS [61].

Another approach is the concept of reviewability, which is introduced as a framework for improving the accountability of ADM involving machine learning. This approach views ADM as a socio-technical process involving both human and technical elements, beginning before a decision is made and extending beyond the decision itself [45].

In conclusion, the establishment of auditing and certification mechanisms tailored to ADMS is a promising avenue for ensuring ongoing compliance and accountability. However, it's important to note that these mechanisms should be designed and implemented carefully, considering the various challenges and complexities involved.

IX. Conclusion

In conclusion, this comprehensive exploration of GDPR compliance in ADMS illuminates the intricate landscape where technology, ethics, and legal considerations intersect. As our world becomes increasingly reliant on automated systems, the imperative to navigate this terrain responsibly and ethically has never been more vital.

The key findings underscore the paramount importance of GDPR in shaping the ethical dimensions of ADM. It transcends mere legal compliance, acting as a beacon that guides organisations, regulators, and individuals toward a future where technological advancements coexist harmoniously with fundamental human rights.

The journey through the GDPR Compliance Framework revealed the critical role of transparency, fairness, and accountability in shaping responsible data processing practices. The intricacies of DPIAs emerged as essential tools in ensuring that the deployment of ADMS aligns with the principles laid out in GDPR.

Challenges in compliance, such as transparency, explainability, and algorithmic bias, surfaced as hurdles that demand innovative solutions. Yet, in these challenges, there lies an opportunity for organisations to pioneer ethical approaches that not only meet regulatory requirements but also foster trust among users and stakeholders.

The exploration of compliance strategies brought forth inspiring case studies and examples of successful efforts, emphasizing the significance of privacy by design and default. organisations that integrate these principles into their decision-making processes not only enhance their resilience against legal consequences but also contribute to a culture that values privacy and individual rights.

The legal and ethical implications of GDPR non-compliance highlighted the connectivity of legal obligations and ethical responsibilities. Beyond avoiding penalties, organisations must recognize their moral duty to safeguard individuals' rights and navigate the ethical complexities inherent in ADM.

The impact on individuals, as safeguarded by GDPR, unveils a landscape where rights to access, rectify, and object to automated decisions empower individuals in the digital realm. However, concerns surrounding autonomy and decision-making underscore the need for ongoing vigilance to ensure that technological progress does not infringe upon individual freedoms.

As we peer into the future trends and developments, the assignment anticipates the continued evolution of technology and its impact on compliance and decision-making. The rise of emerging technologies beckons a proactive approach, where stakeholders collaborate to shape a future where ethical considerations seamlessly integrate into the fabric of automated systems.

In summary, this assignment serves as a compass in the ethical frontier of ADM, emphasizing the symbiotic relationship between GDPR compliance and responsible technological innovation. The insights gleaned from this exploration reinforce the notion that, in the age of automation, ethics must be ingrained in the very fabric of our technological advancements. By prioritizing transparency, fairness, and data protection, we can collectively pave the way for a future where ADM processes align with our shared values and respect for individual rights.

References

[1] Consequences of gdpr non-compliance — gdprhandbook. https://www.gdprhandbook.eu/consequenses-gdpr. (Accessed on 22/11/2023).

[2] Data security, privacy and governance - dporganizer. https://www.dporganizer.com/. (Accessed on 17/11/2023).

[3] Ethical ai frameworks, guidelines, toolkits — ai ethicist. https://www.aiethicist.org/frameworks-guidelines-toolkits. (Accessed on 24/11/2023).

[4] Eur-lex - 31995l0046 - en - eur-lex. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX (Accessed on 09/11/2023).

[5] Eur-lex - 32016r0679 - en - eur-lex. https://eur-lex.europa.eu/eli/reg/2016/679/oj. (Accessed on 09/11/2023).

[6] Pros, inc. a delaware corporation - investor relations. https://ir.pros.com/overview/default.aspx. (Accessed on 17/11/2023).

[7] What is gdpr, the eu's new data protection law? - gdpr.eu. https://gdpr.eu/what-is-gdpr/. (Accessed on 09/11/2023).

[8] Art. 14 gdpr – information to be provided where personal data have not been obtained from the data subject - general data protection regulation (gdpr). https://gdpr-info.eu/art-14-gdpr/, October 2016. (Accessed on 22/11/2023).

[9] Art. 18 gdpr – right to restriction of processing - general data protection regulation (gdpr). https://gdpr-info.eu/art-18-gdpr/, August 2016. (Accessed on 22/11/2023).

[10] Art. 17 gdpr – right to erasure ('right to be forgotten') - general data protection regulation (gdpr). https://gdpr-info.eu/art-17-gdpr/, June 2017. (Accessed on 22/11/2023).

[11] Art. 13 gdpr – information to be provided where personal data are collected from the data subject - general data protection regulation (gdpr). https://gdpr-info.eu/art-13-gdpr/, August 2018. (Accessed on 22/11/2023).

[12] Art. 15 gdpr – right of access by the data subject - general data protection regulation (gdpr). https://gdpr-info.eu/art-15-gdpr/, March 2018. (Accessed on 22/11/2023).

[13] Art. 16 gdpr – right to rectification - general data protection regulation (gdpr). https://gdpr-info.eu/art-16-gdpr/, March 2018. (Accessed on 22/11/2023).

[14] Art. 20 gdpr – right to data portability - general data protection regulation (gdpr). https://gdpr-info.eu/art-20-gdpr/, March 2018. (Accessed on 22/11/2023).

[15] Art. 22 gdpr – automated individual decision-making, including profiling - general data protection regulation (gdpr). https://gdpr-info.eu/art-22-gdpr/, July 2018. (Accessed on 10/11/2023).

[16] Art. 4 gdpr – definitions - general data protection regulation (gdpr). https://gdpr-info.eu/art-4-gdpr/, March 2018. (Accessed on 22/11/2023).

[17] Automated decision-making and profiling — european data protection board. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/automated-decision-making-and-profiling_en, May 2018. (Accessed on 10/11/2023).

[18] Data minimisation - gdpr summary. https://www.gdprsummary.com/gdpr-definitions/data-minimisation/, December 2018. (Accessed on 16/11/2023).

[19] Profiling: The challenges of the gdpr - schürmann rosenthal dreyer lawyers schürmann rosenthal dreyer lawyers. https://www.srd-rechtsanwaelte.de/en/blog/profiling-challenges/, August 2019. (Accessed on 22/11/2023).

[20] Recital 60 - information obligation - general data protection regulation (gdpr). https://gdpr-info.eu/recitals/no-60/, September 2019. (Accessed on 22/11/2023).

[21] Gdpr individual data rights and access. https://www.gdpreu.org/the-regulation/list-of-data-rights/right-of-access/, July 2020. (Accessed on 22/11/2023).

[22] Art. 5 gdpr – principles relating to processing of personal data - general data protection regulation (gdpr). https://gdpr-info.eu/art-5-gdpr/, October 2021. (Accessed on 23/11/2023).

[23] European convention on human rights - article 8 — european union agency for fundamental rights. https://fra.europa.eu/en/law-reference/european-convention-human-rights-article-8-0, March 2022. (Accessed on 23/11/2023).

[24] Gdpr compliance case study — managing the responsibility of gdpr. https://onspring.com/insights/managing-the-responsibilities-of-gdpr-compliance/, July 2022. (Accessed on 17/11/2023).

[25] What is data minimization? https://www.natlawreview.com/article/data-minimization-what-it-and-why-practice-it, February 2022. (Accessed on 24/11/2023).

[26] Art. 6 gdpr – lawfulness of processing - general data protection regulation (gdpr). https://gdpr-info.eu/art-6-gdpr/, January 2023. (Accessed on 23/11/2023).

[27] Automated decision-making and society - the university of sydney law school. https://www.sydney.edu.au/law/our-research/research-centres-and-institutes/automated-decision-making-and-society–.html, May 2023. (Accessed on 10/11/2023).

[28] Automated decision-making impacting society — knowledge for policy. https://knowledge4policy.ec.europa.eu/foresight/automated-decision-making-impacting-society_en, February 2023. (Accessed on 10/11/2023).

[29] Gdpr challenges in the age of ai. https://www.linkedin.com/pulse/gdpr-challenges-age-ai-cresco-business-law-firm/, October 2023. (Accessed on 12/11/2023).

[30] A guide to the data protection principles — ico. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/, July 2023. (Accessed on 22/11/2023).

[31] How do we do a dpia? — ico. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/, May 2023. (Accessed on 17/11/2023).

[32] Navigating automated decision-making: Ensuring gdpr compliance - gdpr advisor. https://www.gdpr-advisor.com/automated-decision-making/, March 2023. (Accessed on 10/11/2023).

[33] What is automated individual decision-making and profiling? — ico. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/automated-decision-making-and-profiling/what-is-automated-individual-decision-making-and-profiling/, May 2023. (Accessed on 09/11/2023).

[34] What is human-ai collaboration? - ai university. https://ai.university/what-is-human-ai-collaboration/, June 2023. (Accessed on 24/11/2023).

[35] KLABUNDE Achim. Guidelines on the protection of personal data in it governance and. March 2018. (Accessed on 09/11/2023).

[36] Ahmet Bilal Aytekin. Algorithmic bias in the context of european union anti-discrimination directives. 2022. (Accessed on 12/11/2023).

[37] Saurabh Bagchi. What is a black box? a computer scientist explains what it means when the inner workings of ais are hidden. https://techxplore.com/news/2023-05-black-scientist-ais-hidden.html, May 2023. (Accessed on 12/11/2023).

[38] Sandra Barbosa and Sara Félix. Algorithms and the gdpr: An analysis of article 22. https://protecaodedadosue.cedis.fd.unl.pt/wp-content/uploads/2022/10/3.-Sandra-Barbosa.pdf, 2022. (Accessed on 12/11/2023).

[39] Sebastião Barros Vale and Gabriela Zanfir-Fortuna. Automated decision-making under the gdpr: Practical cases from courts and data protection authorities. In *Future of Privacy forum*, May 2022. (Accessed on 22/11/2023).

[40] Sebastião Barros Vale and Gabriela Zanfir-Fortuna. Fpf report: Automated decision-making under the gdpr - a comprehensive case-law analysis - future of privacy forum. https://fpf.org/blog/fpf-report-automated-decision-making-under-the-gdpr-a-comprehensive-case-law-analysis/, August 2023. (Accessed on 23/11/2023).

[41] Lou Blouin. Ai's mysterious 'black box' problem, explained — university of michigan-dearborn. https://umdearborn.edu/news/ais-mysterious-black-box-problem-explained, March 2023. (Accessed on 12/11/2023).

[42] Matt Burgess. What is gdpr? the summary guide to gdpr compliance in the uk — wired uk. https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018, March 2020. (Accessed on 09/11/2023).

[43] Srinivasa Rao Chalamala, Naveen Kumar Kummari, Ajeet Kumar Singh, Aditya Saibewar, and Krishna Mohan Chalavadi. Federated learning to comply with data protection regulations. *CSI Transactions on ICT*, 10(1):47–60, 2022. (Accessed on 23/11/2023).

[44] Daoud Chami Christopher Danz. Eu ai act: How explainable ai simplifies regulatory compliance. https://positivethinking.tech/insights/navigating-the-eu-ai-act-how-explainable-ai-simplifies-regulatory-compliance/, June 2023. (Accessed on 23/11/2023).

[45] Jennifer Cobbe, Michelle Seng Ah Lee, and Jatinder Singh. Reviewable automated decision-making: A framework for accountable algorithmic systems. In *Proceedings of the 2021 ACM conference on fairness, accountability, and transparency*, pages 598–609, March 2021. (Accessed on 24/11/2023).

[46] Alessandro Sorniotti Daniel Thyssen. Blockchain for sensitive and personal data. https://www.openaccessgovernment.org/blockchain-sensitive-personal-data/40003/, November 2017. (Accessed on 23/11/2023).

[47] Shay Danon. Gdpr-privacy by design and by default — deloitte switzerland. https://www2.deloitte.com/ch/en/pages/risk/articles/gdpr-privacy-by-design-and-by-default.html, January 2018. (Accessed on 17/11/2023).

[48] Jacob Dexe, Ulrik Franke, Kasia Söderlund, Niels van Berkel, Rikke Hagensby Jensen, Nea Lepinkäinen, and Juho Vaiste. Explaining automated decision-making: a multinational study of the gdpr right to meaningful

information. *The Geneva Papers on Risk and Insurance-Issues and Practice*, 47(3):669–697, May 2022. (Accessed on 09/11/2023).

[49] Nora Ellis. The top challenges of gdpr every business must tackle. https://www.theknowledgeacademy.com/blog/challenges-of-gdpr/, June 2023. (Accessed on 12/11/2023).

[50] ePrivacy GmbH. Federated learning– new opportunities for data protection compliance – eprivacy blog. https://blog.eprivacy.eu/?p=1348, May 2022. (Accessed on 23/11/2023).

[51] Michèle Finck and Asia Biega. Reviving purpose limitation and data minimisation in personalisation, profiling and decision-making systems (january 11, 2021). *Max Planck Institute for Innovation & Competition Research Paper*, (21-04), March 2021. (Accessed on 24/11/2023).

[52] Abigail Goldsteen, Gilad Ezov, Ron Shmelkin, Micha Moffie, and Ariel Farkash. Data minimization for gdpr compliance in machine learning models. *AI and Ethics*, pages 1–15, September 2021. (Accessed on 16/11/2023).

[53] Jyotsana Gupta. Gdpr compliance challenges of ai projects and how to solve them — latest digital transformation trends — cloud news — wire19. https://wire19.com/gdpr-compliance-challenges-of-ai-projects/, September 2022. (Accessed on 12/11/2023).

[54] Lauren Hansen. What is explainable ai (xai)? — enterprise networking planet. https://www.enterprisenetworkingplanet.com/data-center/explainable-ai/, January 2022. (Accessed on 23/11/2023).

[55] Margot E Kaminski and Gianclaudio Malgieri. Algorithmic impact assessments under the gdpr: producing multi-layered explanations. *International Data Privacy Law*, 11(2):125–144, April 2021. (Accessed on 17/11/2023).

[56] Tim Keary. Experts highlight how automated decision-making can violate gdpr — venturebeat. https://venturebeat.com/security/automated-decision-gdpr/, May 2022. (Accessed on 16/11/2023).

[57] Joe McKendrick and Andy Thurai. Ai isn't ready to make unsupervised decisions. https://hbr.org/2022/09/ai-isnt-ready-to-make-unsupervised-decisions, September 2022. (Accessed on 10/11/2023).

[58] Tim T. Mercer. The impact of technology and automation on today's businesses. https://www.forbes.com/sites/forbesbooksauthors/2021/03/25/the-impact-of-technology-and-automation-on-todays-businesses/, March 2021. (Accessed on 10/11/2023).

[59] CRISC CDPSE CIPM Six Sigma Certified Green Belt Mohammed Khan, CISA. Data minimization—a practical approach. https://www.isaca.org/resources/news-and-trends/industry-news/2021/data-minimization-a-practical-approach, March 2021. (Accessed on 24/11/2023).

[60] Jakob Mökander and Maria Axente. Ethics-based auditing of automated decision-making systems: intervention points and policy implications. *AI & SOCIETY*, 38(1):153–171, October 2021. (Accessed on 09/11/2023).

[61] Jakob Mökander, Jessica Morley, Mariarosaria Taddeo, and Luciano Floridi. Ethics-based auditing of automated decision-making systems: Nature, scope, and limitations. *Science and Engineering Ethics*, 27(4):44, July 2021. (Accessed on 24/11/2023).

[62] Margarita Młodziejewska and Henning Soller. Putting data ethics into practice. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/tech-forward/putting-data-ethics-into-practice, February 2023. (Accessed on 09/11/2023).

[63] Andreas Kremer Raj Dash and Aleksander Petrov. Designing next-generation credit-decisioning models — mckinsey. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/designing-next-generation-credit-decisioning-models, December 2021. (Accessed on 09/11/2023).

[64] Michael Ross and James Taylor. Managing ai decision-making tools. https://hbr.org/2021/11/managing-ai-decision-making-tools, November 2021. (Accessed on 10/11/2023).

[65] Shabnam Tai. Automated decision making regulations: An explanation of privacy rules. https://blog.independent.org/2022/06/09/automated-decision-making-privacy-regulations/, June 2022. (Accessed on 21/11/2023).

[66] Howard Womersley Smith Christian Leuthner Asha Sharma Barbara Li Amy Yin Sarah L. Bruno Bryan Tan. Blockchain and data protection – an faq guide — perspectives — reed smith llp. https://www.reedsmith.com/en/perspectives/2022/11/blockchain-and-data-protection–an-faq-guide, November 2022. (Accessed on 23/11/2023).

[67] Upen. What is the difference between legal compliance and ethical responsibility - pediaa.com. https://pediaa.com/what-is-the-difference-between-legal-compliance-and-ethical-responsibility/, February 2019. (Accessed on 22/11/2023).

[68] Sebastião Barros Vale. Gdpr and the ai act interplay: Lessons from fpf's adm case-law report - future of privacy forum. https://fpf.org/blog/gdpr-and-the-ai-act-interplay-lessons-from-fpfs-adm-case-law-report/, November 2022. (Accessed on 09/11/2023).

[69] Patrick Weber, K Valerie Carl, and Oliver Hinz. Applications of explainable artificial intelligence in finance—a systematic review of finance, information systems, and computer science literature. *Management Review Quarterly*, pages 1–41, February 2023. (Accessed on 23/11/2023).

[70] Elin Wihlborg, Hannu Larsson, and Karin Hedström. "the computer says no!"–a case study on automated decision-making in public authorities. In *2016 49th Hawaii International Conference on System Sciences (HICSS)*, pages 2903–2912. IEEE, 2016. (Accessed on 17/11/2023).