AI Profiling in the EU: *A Critical Analysis for AI Governance in Japan*

By: David U. Socol de la Osa
For: Center for International Economic Collaboration (CFIEC)

Table of Contents

AI PROFILING IN THE EU: *A Critical Analysis for AI Governance in Japan*

By: David U. Socol de la Osa
For: Center for International Economic Collaboration (CFIEC)

1. INTRODUCTION

1.1 Overview of the Research Question and Objectives

This report investigates the concept of profiling and its treatment under European Union (EU) regulations, particularly through the lens of artificial intelligence (AI) systems deployment. AI-driven profiling holds significant implications, as it leverages vast amounts of data to infer and predict individual behavior, raising complex questions about its impact on privacy, fairness, and fundamental rights. The report aims to explore key EU regulations governing profiling and assess how these regulations address AI-specific issues at multiple levels: business, social, and political. Building on this analysis, the report will offer actionable recommendations for Japan on effectively regulating AI-profiling.

The report has the following framework and objectives:

- **Scope**: Profiling in relation to AI systems
- **Target jurisdiction**: European Union
- **Target sectors**: Business, social, and political
- **Objective**: By analyzing the EU's response to AI profiling, the report aims to develop recommendations for Japan

Annex I provides a summary of the documents analyzed, outlining their key features and their impact on AI profiling. **Annex II** contains findings and advisory measures, with foundational considerations detailed in Annex II.1 and regulatory recommendations outlined in Annex II.2.

1.2 Significance of Profiling and AI Governance: Insights from the EU and Implications for Japan

AI & Profiling: In the age of AI, profiling has gained critical importance due to the increasing scope, scale, depth, applicability, and socio-technological complexity of the relationship between profiling practices and AI systems. AI profiling processes have tremendous potential for societal impact and demographic extension, and often operate in opaque ways, magnifying risks such as algorithmic bias, data misuse, and infringements on privacy rights. AI-driven profiling has complex interactions with many legacy legal principles, including the rights and liberties afforded to EU citizens. These issues are particularly pronounced in multi-sectoral contexts—business, social, and political—where profiling can influence decision-making on individual and societal levels. In response to these risks, the EU's regulatory standards provide a valuable model for addressing profiling challenges and fostering trust in AI systems.

The EU as a Target Jurisdiction: The EU's regulatory framework for profiling serves as a global benchmark due to its comprehensive approach and emphasis on safeguarding human rights, democracy, and the rule of law. The EU has been at the forefront of regulating profiling, particularly through documents such as the **General Data Protection Regulation (GDPR)** and the **AI Act**, which collectively and in a multi-vector manner address the complexities of AI-driven profiling.

The Future of AI Profiling in Japan: As Japan navigates unique and particular challenges in AI governance, the EU's profiling regulation can offer valuable insights. Japan's commitment to AI-driven innovation, and its position as a major economy and technological development and implementation hub, requires robust and precise governance frameworks to address the ethical, legal, and social implications of profiling. By examining the EU's regulatory structures, Japan can identify effective strategies for harmonizing innovation with societal values, particularly in contexts where data-driven technologies intersect with human rights and democracy.

1.3 Structure of the report

This report (i) provides a comprehensive overview of the legal framework governing AI-profiling in the EU, focusing on key legislation, and (ii) the report develops targeted recommendations for Japan, informed by the insights gained. The structure of the report is as follows:

LEGAL FRAMEWORK OF PROFILING

- **Overview of Profiling**: Definition, scope, and significance of profiling in the context of AI systems in the EU.
- **Legal Analysis of Key EU Governance Documents:** A comprehensive examination of critical EU legislation, focusing on (i) the defining features and frameworks of each regulatory instrument, and (ii) their implications across three distinct perspectives: business, social, and political. The analysis will encompass the following documents:
    - General Data Protection Regulation (GDPR)
    - AI Act (Artificial Intelligence Act)
    - Digital Services Act (DSA)
    - Digital Markets Act (DMA)
    - Right-to-Repair Directive
    - Unfair Commercial Practices Directive
    - Data Act
    - Commission Staff Working Document: Fitness Check of EU Consumer Law on Digital Fairness

RECOMMENDATIONS AND BEST PRACTICES FOR JAPAN: Practical, actionable insights drawn from EU regulatory frameworks, specifically adapted to align with Japan's governance landscape and policy objectives.

1.4 Executive Summary

AI-driven profiling is increasingly shaping economic, social, and political interactions, raising fundamental challenges for governance, privacy, fairness, and accountability. As AI systems process vast amounts of personal data to predict behavior and automate decision-making, ensuring transparency, user control, and regulatory oversight has become paramount. This has raised significant regulatory questions on how to balance technological development, economic competitiveness, and fundamental rights.

*A summary of the documents analyzed, their key features and their impact on AI profiling, can be found in **Annex I**. Findings and advisory, including foundational considerations, and regulatory recommendations, can be found in **Annex II.1 and II.2** respectively.*

This report examines the European Union's (EU) regulatory approach to AI-driven profiling, analyzing key legislative frameworks such as the **General Data Protection Regulation (GDPR), Artificial Intelligence Act (AI Act), Digital Services Act (DSA), Digital Markets Act (DMA), Unfair Commercial Practices Directive (UCPD), and Data Act**. These instruments collectively address the risks and opportunities of profiling, balancing innovation with consumer protection, market fairness, and individual rights.

The report is structured around three major sectorial dimensions where AI profiling plays a critical role:

- *Business*: AI profiling significantly impacts economic interactions, including driving targeted advertising, dynamic pricing, credit scoring, and employment decisions, necessitating safeguards against manipulation, bias, and exploitative personalization.
- *Social*: The use of profiling in sectors such as healthcare, education, and law enforcement presents challenges of discrimination, systemic bias, and inequitable access to essential services.
- *Political*: The political arena is increasingly affected by AI-based individual assessments, with algorithmic content targeting, voter profiling, and automated misinformation risks pose serious threats to democratic processes and public trust in institutions.

Building on EU regulatory frameworks, this report presents two core components for Japan's AI-profiling governance: (1) **Foundational considerations** and (2) **regulatory recommendations**. The foundational considerations outline key principles to balance innovation, economic growth, and fundamental rights while ensuring AI-driven profiling remains transparent, accountable, and fair. These include adopting an actionable rights-based approach, promoting regulatory agility, designing sector-specific approaches with public-private partnerships, developing the data economy, ensuring accountability in both the public and private sectors AI-profiling, and fostering international cooperation.

The recommendations translate these principles into concrete regulatory measures, focusing on **enhancing individual rights and data control**, including protections for sensitive data and vulnerable populations, and establishing a **proportional, risk-based compliance model** that imposes stricter obligations on high-risk profiling and data-dominant entities while maintaining flexibility for smaller businesses. Additionally, they call for **clear safeguards on corporate and government profiling**, responsible data-sharing frameworks that prevent monopolization while fostering economic growth, and regulations to mitigate manipulative AI-driven personalization and dark patterns. The report further emphasizes **lifecycle compliance mechanisms**, including pre-market certification, regular auditing, and adaptive oversight, alongside strengthened **international cooperation** to align Japan's AI governance with global standards and democratic leadership while maintaining national data autonomy.

As Japan refines its AI governance framework, aligning with global best practices while accounting for its unique technological and economic landscape will be crucial in ensuring responsible AI deployment. This report serves as a roadmap for developing a legal architecture that fosters AI innovation while protecting individual autonomy, fairness, and democratic integrity.

2. Legal Framework of Profiling in the EU

This section provides an in-depth overview of the general framework governing AI profiling within the European Union. Profiling in the EU is regulated through a multifaceted legal landscape, balancing technological innovation with the protection of fundamental rights. The section explores the key legal instruments and principles shaping profiling regulations, focusing on their role in addressing privacy, fairness, and accountability.

The analysis unfolds in four parts:

1. **Definition and Context** – Examines the legal definition of profiling under EU law and its application across various regulatory frameworks, including the GDPR.
2. **General Structure** – Outlines the core regulatory mechanisms and governance frameworks underpinning profiling, highlighting the interplay between EU legislation and member states' responsibilities.
3. **Key Features and Governance Provided by the GDPR** – Discusses the GDPR's principles, safeguards, and specific provisions governing profiling, including its focus on automated decision-making and sensitive data.
4. **Placement Within the Multi-Jurisdictional Context of the EU** – Explores how the EU harmonizes diverse legal systems while maintaining flexibility for member states to address national priorities.

2.1 Defining Profiling in the EU: A Balancing Act Between Data and Rights

2.1.1 General Definition of Profiling, and the Rise of AI

Profiling, as defined by the **European Union Agency for Fundamental Rights**, involves categorizing individuals based on their characteristics.[1] This process requires the collection of data and subsequent actions informed by the identification of specific traits or attributes.

When integrated with AI, profiling takes on a new dimension of complexity and risk. The automated processing of data by AI systems amplifies concerns about privacy, fairness, and the erosion of individuality. Unlike traditional forms of profiling, AI-driven profiling operates at unprecedented scales and speeds, analyzing vast datasets to infer patterns, predict behaviors, or classify individuals. These capabilities often lack transparency, making it difficult for individuals to understand how decisions about them are being made, potentially being consequent to protected categories of data, or infringing upon their privacy.

[1] European Union Agency for Fundamental Rights, Preventing Unlawful Profiling Today and in the Future: A Guide (2018), available at https://fra.europa.eu/en/publication/2018/preventing-unlawful-profiling-today-and-future-guide.

Such automation introduces significant risks to rights and freedoms. Decisions based on AI profiling can perpetuate biases, discriminate against vulnerable groups, or reduce individuals to a set of data points. The potential for harm extends across all aspects of life—economic opportunities, social participation, and political engagement.

This is why the EU has prioritized robust regulatory measures to address profiling, ensuring that individuals' fundamental rights are upheld in the face of advancing technology. Laws like the GDPR and the AI Act impose strict safeguards, demanding transparency, fairness, and human oversight in AI profiling systems. By emphasizing accountability and the protection of individual freedoms, these regulations aim to balance technological innovation with the ethical and societal values central to European governance.

2.1.2 Profiling Under EU Law: Fragmentation Across Legislation

Within the European Union, profiling is not governed by a single, unified legal definition or framework. Instead, its regulation is fragmented across multiple pieces of legislation, each addressing profiling in specific contexts. Key regulations to be analyzed in this report include:

- General Data Protection Regulation (GDPR)
- AI Act (Artificial Intelligence Act)
- Digital Services Act (DSA)
- Digital Markets Act (DMA)
- Right-to-Repair Directive
- Unfair Commercial Practices Directive
- Data Act
- Commission Staff Working Document: Fitness Check of EU Consumer Law on Digital Fairness

This fragmentation reflects the multifaceted nature of profiling in modern governance, as well as its implications across various domains, including business, social, and political sectors. To address this complexity, this report will analyze these laws to identify how they regulate profiling and its associated risks in the context of AI systems.

2.1.3 The GDPR and Profiling Governance

The GDPR serves as a cornerstone in regulating profiling practices. This subsection outlines (i) the definition of profiling under provided by the GDPR, which serves as a core and foundational definition for EU regulation comprehensively; (ii) the safeguards established to govern data processing for profiling purposes; and (iii) the principles of what profiling is permissible under EU regulation.

i. Legal Definition of Profiling

The **General Data Protection Regulation (GDPR)** is a key document for profiling governance in the EU. The GDPR provides a definition of profiling, in its **Article 4(4),** as follows:

> "*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 analyze or predict aspects concerning that natural person's performance at work,*

economic situation, health, personal preferences, interests, reliability, behavior, location, or movements."

The GDPR's definition of profiling is deliberately broad, capturing activities such as predictive analytics and behavioral monitoring. It underscores the ethical and legal concerns tied to using diverse data points—ranging from socioeconomic and professional indicators to health and personal preferences—to evaluate or forecast individual behavior. By explicitly listing these categories, the regulation highlights the extensive scope of profiling practices it governs and the various ways in which personal data can be processed and applied.

ii. Automated Decision-Making and Profiling under Article 22 GDPR: Safeguards and Implications

Article 22 of the GDPR provides individuals with the right not to be subjected to decisions based solely on automated processing, including profiling, where such decisions produce legal effects or similarly significant impacts on their rights or interests. This provision seeks to ensure that human oversight and accountability remain central in cases where the outcomes of automated processing can materially affect individuals.

Some key provisions include the following (1) general prohibition of profiling, (2) exceptions to the general prohibition, (3) required safeguards and human oversight, (4) significant effect prohibition, and (5) special categories of data:

1. **General Prohibition**: *Profiling, in the context of decision-making processes, is generally prohibited.*
   Article 22 establishes a general prohibition on automated decision-making that has legal or similarly significant effects on individuals.[2] This prohibition is rooted in the need to safeguard individual rights in mitigating risks posed by fully automated processes, which can deprive individuals of fundamental protections.
2. **Exceptions**: *There are certain exceptions by which these processes may take place.*
   Automated decision-making is permissible only under the following specific circumstances:[3]
   - **Contractual Necessity**: When the processing is essential for entering into or performing a contract between the data subject and the controller.
   - **Legal Authorization**: When such processing is explicitly authorized by EU or Member State law, provided suitable safeguards are implemented to protect individual rights.
   - **Explicit Consent**: When the individual has provided explicit consent to the processing, ensuring a higher level of personal control over their data.
3. **Required Safeguards, Human Oversight**: *Data subjects have the right to human intervention to safeguard rights and legitimate interests*.
   In cases where exceptions apply, the GDPR mandates specific safeguards to protect individuals, anchored by the right to obtain human intervention, with a process to contest

[2] GDPR Art 22(1).
[3] GDPR Art 22(2)(a-c).

decisions made.[4] To meet these requirements, human involvement in decision-making must be meaningful and substantive. Superficial or perfunctory reviews are insufficient; instead, oversight must be capable of overriding automated decisions and based on a thorough understanding of the relevant data.

4. **Significant Effect**: *Profiling associated to decision-making warrants particular attention due to its profound potential to impact individuals' rights, freedoms, and overall life trajectories.*
   A legal effect under Article 22 GDPR arises when a decision based solely on automated processing significantly impacts an individual's legal rights, status, or fundamental liberties. These include actions and freedoms that affect business, social, and political spheres, such as voting rights, access to education, freedom of association, or restrictions on movement due to police interactions. Legal consequences may also include contract termination, denial of social benefits, or refusal of citizenship or admission to a country.

   Automated processing, including profiling, involves analyzing or predicting aspects of an individual's personal life—such as work performance, financial circumstances, health, personal preferences, behavior, or location—that produce legal or similarly significant effects. Examples include the automatic denial of an online credit application or recruitment decisions made without human oversight.[5] While such processing is generally restricted, it is permissible in certain cases, such as when expressly authorized by Union or Member State law (e.g., for fraud prevention), necessary for contract performance, or based on the individual's explicit consent. In all cases, controllers must implement safeguards to protect the data subject, such as the right to human intervention, the ability to contest the decision, and mechanisms to ensure transparency and fairness.

   Although the GDPR does not explicitly define "significant effect," it emphasizes that these effects must meaningfully alter an individual's position, rights, or freedoms.[6] Such protections aim to prevent the misuse of profiling and automated processing, particularly where discriminatory outcomes or systemic biases may arise. To ensure compliance, controllers are required to adopt robust technical and organizational measures, such as correcting inaccuracies, minimizing errors, and securing personal data, while maintaining transparency and accountability throughout the decision-making process.

   While not all automated decisions, such as those involving targeted advertising, may typically meet this threshold, there are cases where profiling can significantly affect individuals. The impact depends on factors such as the intrusiveness of the profiling, the data subjects' expectations, and their vulnerabilities. This is particularly true for marginalized groups, such as minors, minority populations, or vulnerable adults, who may experience disproportionate impacts. Differential pricing based on personal data may also constitute a

[4] GDPR Art 22(3).
[5] GDPR Recital 71.
[6] Id.

significant effect if, for instance, it results in prohibitively high prices that effectively deny access to goods or services.

5. **Special Categories of Data**: *Certain categories of data have elevated protections due to their sensitive or vulnerable nature.*
   Article 22 explicitly prohibits automated decision-making based on sensitive personal data, unless processing is justified under strict legal conditions and accompanied by appropriate safeguards.

   Under the GDPR, personal data encompasses any information that identifies or relates to an individual. "Special categories" are afforded heightened protection due to their sensitive nature. These include data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data used for unique identification, health-related data, and data concerning a person's sex life or sexual orientation.[7] The processing of such data is generally prohibited, reflecting the GDPR's commitment to safeguarding individuals against the heightened risks of discrimination, misuse, or harm associated with these categories.

iii. Permissible Data Processing for Profiling

Under **Article 6 GDPR**, data processing for profiling is only lawful if it meets one of several defined conditions. These include:

i. Obtaining the data subject's explicit consent for specific purposes,
ii. Fulfilling contractual obligations,
iii. Complying with legal requirements,
iv. Protecting vital interests of individuals,
v. Performing tasks in the public interest, or
vi. Pursuing legitimate interests that do not override the rights and freedoms of the data subject.

In addition to these conditions, any processing for purposes beyond the original intent must adhere to strict compatibility assessments. Controllers must consider factors such as the relationship with the data subject, the nature of the data, potential consequences for individuals, and whether appropriate safeguards, such as pseudonymization or encryption, are in place. For public or official tasks, the legal basis for processing must be explicitly defined in Union or Member State law, ensuring proportionality and alignment with public interest objectives.

These provisions establish a structured framework to ensure that profiling aligns with the GDPR's core principles of lawfulness, fairness, and transparency. They seek to protect data subjects from unjustified risks while enabling necessary or operationally efficient processing in clearly defined contexts.

[7] GDPR Art 9(1).

2.1.4 The EU's Role: Supra-Nationality and Delegation

The EU's regulatory framework for profiling highlights its **supra-national authority** and ability to delegate responsibilities among member states. By setting common standards, the EU seeks to harmonize protections across diverse jurisdictions while enabling member states to address national specificities. This approach underscores the EU's pivotal role in balancing technological innovation with fundamental rights.

3. AI Profiling in the EU: Business, Social, and Political Perspectives

This section examines key EU laws governing AI profiling, analyzing their objectives, provisions, and implications across three critical sectors: business, social, and political.
For each piece of selected key legislation related to AI profiling, the report provides the following:

- **Characteristics of the Law:**
  - A summary of the law's objectives and scope, with a focus on its approach to addressing profiling and associated risks.
  - Identification and analysis of relevant articles or provisions concerning profiling, highlighting their implications for data processing and rights protection.
- **Sectoral Analysis:**
  - **Business:** Examines the law's impact on economic activities such as marketing, advertising, labor markets, and other sectors that directly engage with individuals at a commercial and socioeconomic level.
  - **Social:** Addresses the law's role in social aspects such as public health and the protection of vulnerable populations (e.g., elderly, minors, religious groups).
  - **Political:** Evaluates the law's measures to engage with political spheres such as voting rights, and prevent election manipulation, particularly targeting individuals or groups.

This structured analysis of each regulation, focusing on its objectives, relevant provisions, and sectoral impacts, provides a comprehensive understanding of how profiling is addressed across the EU's legal landscape. By examining profiling at the business, social, and political levels, the report highlights the multifaceted challenges and risks associated with AI-driven profiling.

3.1 General Data Protection Regulation

The **General Data Protection Regulation (GDPR)** governs profiling through a structured approach to **data management and processing**, recognizing its potential risks and **safeguarding fundamental rights** such as privacy, fairness, and non-discrimination. It establishes clear safeguards to **balance the benefits of profiling with the need to protect individuals**, emphasizing transparency, accountability, and adherence to EU principles.
At its core, the GDPR **governs data gathering, processing, and overall management** to ensure that profiling is conducted responsibly and ethically. It achieves this by **establishing rights** for individuals, such as access to their data and the ability to contest automated decisions, while imposing obligations on organizations to ensure fairness and accountability. Essentially, the

GDPR provides the overarching framework for data protection, and profiling is addressed as a key component within a broader system of rights and responsibilities of data governance.

Below is an overview of how the GDPR applies to profiling, its definition and context, as well as key features:

(1) Defining Features & Characteristics

i. Definition and Context

The **General Data Protection Regulation (GDPR)** explicitly governs profiling as a form of data processing, subject to strict safeguards and limitations. Profiling is subject to GDPR provisions, including legal grounds for processing and data protection principles.[8] Additionally, the **European Data Protection Board (EDPB)** has the authority to issue guidance on profiling to ensure compliance across member states.[9]

Definition of Profiling: The GDPR defines profiling in **Article 4(4)** as:

> "*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*."[10]

This broad definition encompasses a range of activities by data gatherers and processors, from predictive analytics to behavioral monitoring, while emphasizing the significant ethical and legal implications of using a wide variety of data points including socioeconomic, professional, health, and personal items to evaluate or predict aspects of an individual's life. By explicitly including these categories, the definition highlights (i) the breadth of profiling practices governed by the GDPR and (ii) the ample modalities of behaviors covered within the context of personal data covered.

Balancing Rights and Freedoms with Data Processing and Profiling: The GDPR recognizes data processing and profiling as activities that can pose significant risks to the rights and freedoms of individuals.[11] These risks, which vary in likelihood and severity, stem from the potential for physical, material, or non-material harm resulting from personal data misuse.[12] Such harms include discrimination, identity theft, financial loss, reputational damage, unauthorized pseudonymization reversal, and the deprivation of individuals' ability to exercise control over their personal data.

---

[8] GDPR Recital 72.
[9] Id.
[10] GDPR Art 4(4).
[11] GDPR Recital 75.
[12] Id.

The regulation acknowledges that certain types of data—such as information revealing racial or ethnic origin, political opinions, religious beliefs, trade union membership, or data concerning health, genetic information, or sexual life—are particularly sensitive. Processing these categories of data amplifies the risk of harm, especially when personal aspects are evaluated to create or use profiles that predict or analyze characteristics such as work performance, economic situation, health, or behavior. The risk is further exacerbated in cases involving vulnerable groups, such as children, or when processing large volumes of data impacting many individuals.[13]

To address these challenges, the GDPR seeks to strike a balance between the legitimate needs of data processing and the protection of individual rights and freedoms. By implementing principles such as transparency, fairness, accountability, and purpose limitation, the regulation imposes strict safeguards to mitigate harm. These include limiting the scope of data collection, requiring explicit consent for sensitive data, and ensuring that profiling or automated decision-making does not undermine fundamental rights.[14] Through this balancing act, the GDPR aims to enable innovation and data-driven progress while maintaining the dignity and autonomy of individuals in the digital age.

ii. Restrictions on Special Categories of Data

The GDPR imposes heightened requirements for processing **special categories** of personal data due to the significant risks these activities pose to individuals' fundamental rights and freedoms.[15] These categories include data racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data used for unique identification, health data, and data related to a person's sex life or sexual orientation.

General prohibition, exemptions: These categories of data are considered inherently sensitive and, are generally prohibited from processing unless specific exemptions apply.

These exemptions include cases where explicit consent is provided, where processing fulfills legal obligations or protects vital interests, and where it serves substantial public interests, such as public health or social protection.[16] Processing is also allowed for legitimate activities by non-profits, for data made public by the subject, and in the context of legal claims or judicial proceedings. Additionally, sensitive data can be processed for healthcare purposes, scientific research, statistical analysis, or archival purposes, provided that robust measures, such as pseudonymization, are in place to protect data subjects. These provisions ensure that high-risk processing, particularly profiling involving sensitive data, is conducted responsibly and remains aligned with fundamental rights.

---

[13] Id.

[14] See discussion infra Section 2.2.1(1)(iv).

[15] GDPR Art 9.

[16] GDPR Art 9(2), Recital 54.

iii. Scope and Jurisdictionality

The GDPR extends its jurisdiction beyond the physical borders of the EU, regulating personal data processing under defined conditions, including by entities outside the Union targeting individuals within its territory. This section examines the material and territorial scope of the regulation, emphasizing its broad reach and nuanced limitations.

Material Scope: What Does It Cover? *Personal data to be structured*

The GDPR has an extensive material scope, applying to the processing of personal data by automated or manual means, provided the data forms or is intended to form part of a structured filing system.[17] This wide application spans public and private sector activities.

> *Exclusions*: The regulation includes several exclusions, such as processing for personal or household purposes, actions by Member States in specific capacities (e.g., under Chapter 2 of Title V of the TEU), activities outside the remit of EU law, and data processing related to law enforcement and public security.[18] The GDPR does not apply to areas beyond the EU's legislative scope, such as national security or activities under the Union's foreign and security policy. [19]

Territorial Scope: Where Does It Apply? *Data processing (i) by entities established in the EU, (ii) non-EU entities processing or targeting data of persons located within the EU*

The GDPR territorial scope is expansive, as the regulation governs over **data processing by controllers or processors established in the EU**, irrespective of where the processing takes place. Additionally, the regulation applies to **non-EU entities that process the personal data of individuals located within the EU**. This includes situations where entities offer goods or services to individuals in the EU—whether paid or free—or monitor their behavior within EU territory.

> *Intentionality of targeting EU persons*: In order for the GDPR to apply to non-European entities, there must clear intent when targeting EU individuals. These techniques can include marketing in EU languages, pricing in EU currencies, or other tailored strategies.[20] Similarly, monitoring activities, such as profiling individuals to analyze or predict preferences, behaviors, or attitudes, also bring non-EU entities under the GDPR's jurisdiction.[21]

Who Does It Cover? *Natural persons*

The GDPR protects **natural persons**, regardless of their nationality or residence.[22] It does not, however, apply to legal persons, such as corporations. This distinction underscores the

---

[17] GDPR Art 2.

[18] Id.

[19] Id. GDPR Recital 16.

[20] GDPR Recitals 23, 24.

[21] Id.

[22] GDPR Recital 14. European Commission, Data Protection under GDPR, Your Europe, https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_en.htm (last visited Mar. 7, 2025).

regulation's focus on individual rights and its aim to ensure high standards of personal data protection globally.

iv. Rights-Based Approach for Data and Profiling Protection

The GDPR adopts a rights-based approach to safeguard individuals against the risks associated with data processing and profiling. By embedding core principles as actionable items, the regulation ensures that data subjects retain control over their personal information and are protected from harmful or discriminatory outcomes. This section outlines the specific rights and protections guaranteed under the GDPR to uphold these principles, both generally in regards to data, and more specifically pertaining to profiling. The GDPR guarantees several fundamental rights to individuals, including: (1) the right to transparency in how personal data is processed, (2) the right to information and access to one's personal data, (3) the right to rectify inaccuracies or erase personal data under specific circumstances, and (4) the right to object to profiling and automated decision-making that significantly impacts them.

(1) **Transparency:** Data controllers must inform data subjects when profiling occurs, including its purpose, the logic involved, and the potential consequences for them. This ensures that data subjects can understand how their personal data is being used and what impact profiling might have on their rights and privacy.[23]

> *Clarity, special protections*: The GDPR requires that any information provided to data subjects regarding their personal data and processing be clear, concise, and easily understandable. [24] The document underscores the importance of transparency, particularly given the complexity of data practices and the proliferation of actors involved in processing.[25] It highlights the need for plain language and, where appropriate, visual tools, such as standardized icons, to convey essential information.[26] This requirement is particularly relevant for children, who merit additional protections; all communications must be tailored in a manner that allows a child to comprehend the information fully.[27]
>
> *Practical measures*: The regulation emphasizes the practical measures necessary to enable data subjects to exercise their rights effectively.[28] Controllers are obligated to provide mechanisms—free of charge—for individuals to request access, rectification, erasure, or objection to processing. Requests must be addressed without undue delay, typically within one month, and controllers are required to justify any refusal to comply.[29] These provisions ensure that data subjects can maintain meaningful control over their personal data in alignment with the GDPR's core principle of accountability.
>
> *Profiling specifics*: The GDPR builds on this foundation by requiring controllers to inform data subjects about profiling activities, including the purpose and consequences

[23] GDPR Art 12.
[24] GDPR Arts 12-14.
[25] GDPR Recital 58.
[26] Id.
[27] Id.
[28] GDPR Art 12, Recital 59.
[29] GDPR Recital 59.

of such processing.[30] It further mandates that individuals be made aware of whether providing their data is mandatory and the implications of not doing so. This information must be presented in an accessible format, and, when provided electronically, should include machine-readable icons to ensure clarity and usability.

(2) **Information and access to personal data**: The GDPR establishes robust transparency obligations for data controllers when collecting personal data, whether directly from the data subject or from other sources.[31] This is complemented by the right to access, which ensures that individuals can confirm whether their personal data is being processed, review the purposes of the processing, understand the data's intended use, and gain insights into automated decision-making or profiling activities. This right reinforces the principle of transparency by granting individuals meaningful oversight of their personal information.[32]
Controllers must confirm whether processing is occurring, detail its purpose, specify the storage period, disclose recipients, and explain any automated decision-making or profiling. This information enables individuals to understand how their data is used and ensures they remain informed.[33] Access must be straightforward and provided periodically, allowing individuals to review their data and assess its implications. To enhance accessibility, controllers are encouraged to establish secure, remote access systems for data subjects.[34]

Limitations to access: Access rights are not unlimited. Examples of restrictions include infringement upon others' freedoms, trade secrets, or intellectual property, such as software copyrights.[35] While timely and clear communication is emphasized, further exceptions exist where providing information is unnecessary (e.g., if the data subject already has it), impractical (e.g., in large-scale or historical research projects), or explicitly mandated by law. These provisions reflect the GDPR's effort to balance transparency with practical feasibility.[36]

(3) **Rectification and erasure:** Data subjects have the right to correct inaccurate or incomplete data used in profiling, ensuring that decisions are not based on flawed information, and being able to contest processing generally. This is built into the GDPR by way of the rights to (i) rectify, (ii) erase, (iii) restrict processing, (iv) have portable data.[37]

Right to rectification: The right to rectification ensures that individuals can correct inaccurate or incomplete personal data without undue delay.[38] This includes the ability to provide supplementary statements to complete data where necessary. This right is

[30] GDPR Recital 60.
[31] GDPR Arts 13, 14. Controllers must provide individuals with clear and detailed information about data processing at the time of collection or, if the data is obtained indirectly, within a reasonable timeframe. This includes the controller's identity, the purposes of processing, the legal basis, and any intended transfers to third countries.
[32] GDPR Art 15.
[33] Id.
[34] GDPR Recital 63.
[35] GDPR Recital 63.
[36] GDPR Recitals 61, 62.
[37] GDPR Arts 16-20.
[38] GDPR Art 16.

integral to maintaining data accuracy and fairness, preventing decisions based on flawed or incomplete information.[39]

Right to Erasure ('Right to Be Forgotten'): The right to erasure allows data subjects to request the deletion of their personal data under specific conditions, such as when the data is no longer necessary, consent has been withdrawn, or the data was unlawfully processed.[40] This right is particularly relevant when data subjects provided consent as minors or when personal data poses risks if retained.[41] Controllers must also take reasonable steps to inform other controllers of the request to delete publicly shared data. Exceptions exist for reasons such as freedom of expression, legal obligations, public health, and archiving purposes.[42]

Right to Restriction of Processing: This right enables individuals to limit the processing of their data in specific scenarios, such as contesting the accuracy of data, unlawful processing where erasure is not requested, or when the data is required for legal claims.[43]

Right to Data Portability: Data subjects have the right to receive their personal data in a structured, commonly used, and machine-readable format and transfer it to another controller without hindrance.[44] This applies to data processed based on consent, contractual necessity, or automated means.

(4) **Right to object and not be subject to profiling, automated decision-making**: Data subjects can object to profiling and have the right not to be subject to decisions made solely on automated processing, including profiling, if such decisions produce legal or similarly significant effects. Exceptions exist, but safeguards—such as the right to obtain human intervention and challenge decisions—must always be in place.[45]

v. Data Protection Impact Assessment

Data Protection Impact Assessments (DPIAs) are central to the GDPR's approach to mitigating the risks associated with profiling and other high-risk data processing activities. By requiring controllers to proactively evaluate the potential impacts of processing on individuals' rights and freedoms, DPIAs serve as critical tools to prevent harm, ensure compliance, and enhance accountability in data governance.

Key Requirements of DPIAs: The GDPR mandates a DPIA whenever data processing, particularly with new technologies, is likely to result in a high risk to individuals.[46] This includes systematic profiling, large-scale processing of sensitive data, and public monitoring. The DPIA

[39] GDPR Recital 65.
[40] GDPR Art 17.
[41] GDPR Recital 65.
[42] Id.
[43] GDPR Art 18.
[44] GDPR Art 20.
[45] See discussion supra Section 2.1.3(B).
[46] GDPR Art 35.

must systematically analyze the scope, context, and purpose of the processing, assess risks to data subjects, and identify safeguards to mitigate these risks.[47]

Profiling and High-Risk Activities, Mandatory DPIAs: A Data Protection Impact Assessment (DPIA) is mandatory under the GDPR in the following high-risk scenarios:[48]

- **Automated Decision-Making and Profiling**: When personal aspects of individuals are systematically and extensively evaluated through automated processing, including profiling, leading to decisions with legal effects or similarly significant impacts.
- **Large-Scale Processing of Sensitive Data**: When special categories of personal data (e.g., racial or ethnic origin, health data)[49] or data related to criminal convictions and offenses[50] are processed on a large scale.
- **Systematic Monitoring of Public Areas**: When large-scale, systematic monitoring of publicly accessible spaces is conducted, such as through surveillance systems.

Other high-risk processing that may require DPIAs are automated evaluations of personal aspects (e.g., reliability, behavior, or preferences) that significantly impact individuals, such as determining creditworthiness or job eligibility. The GDPR emphasizes that DPIAs are essential for large-scale processing involving sensitive data, biometric data, or criminal records, especially when such activities limit individuals' ability to exercise their rights.[51]

vi. Data Protection Officer

The GDPR creates the figure of a **Data Protection Officer (DPO)**, which plays a critical role in ensuring compliance with data protection regulations, including preventing harmful profiling practices. The DPO is responsible for monitoring an organization's adherence to data protection rules, advising on compliance measures, and serving as a point of contact for supervisory authorities and data subjects. This function is particularly significant in high-risk processing activities such as profiling, where ensuring lawful and fair processing is essential.

Designation of a DPO: A DPO must be appointed in the following cases:[52]

- **Public Authorities**: When the organization is a public authority or body, excluding courts acting in a judicial capacity.
- **Large-Scale Monitoring**: When the core activities involve regular and systematic large-scale monitoring of individuals, such as tracking or profiling.
- **Sensitive Data Processing**: When the core activities include large-scale processing of sensitive data (e.g., health, ethnicity, or criminal records) as defined under Articles 9 and 10 of the GDPR.

[47] GDPR Art 35(1).
[48] GDPR Art 35(3).
[49] GDPR Art 9(1).
[50] GDPR Art 10.
[51] GDPR Recital 91.
[52] GDPR Art 37(1).

Role and Relevance to Profiling: DPOs are tasked with ensuring compliance in high-risk areas like automated decision-making and profiling.[53] By monitoring internal practices, the DPO helps prevent misuse of personal data, including in activities like large-scale profiling, and ensures safeguards are in place to protect individuals.

vii. Sanctions for Non-Compliance

Organizations that fail to comply with the GDPR's rules on profiling may face significant penalties, with fines of up to **€20 million or 4% of global annual turnover**, whichever is higher.[54]

(2) Sectorial Classification

Profiling under the GDPR is regulated to mitigate risks and protect fundamental rights. The framework the GDPR creates, addresses data processing and controlling for individuals within the EU, as well as for entities established in the EU, covering a wide range of jurisdictional reach. Core principles are the rights-based approach anchored by consent and interaction between the data subject and the data gathered, heightened scrutiny for sensitive data, and specific processing situations.

i. Business

The GDPR establishes clear standards for profiling in business contexts, particularly in marketing, employment, and consumer transactions**:**

- **Marketing and Consumer Profiling:** The GDPR provides individuals the right to object to profiling for direct marketing purposes, [55] emphasizing transparency and accountability in the collection and use of consumer data.[56] Profiling children for marketing purposes requires heightened safeguards due to their limited understanding of data risks.[57]
- **Legitimate Interests:** Businesses may process data for legitimate interests, including marketing, provided these interests do not override the rights and freedoms of data subjects, particularly when children are involved.[58] However, the GDPR underscores the need for a careful assessment of whether the data subject could reasonably expect such processing, based on the context and purpose of data collection.[59]
- **Employment Context:** The GDPR provides ample competency to Member States to set their own rules for employee data processing.[60] This includes data profiling in activities such as recruitment, performance evaluation, equality and diversity in the workplace,

[53] Id. GDPR Recital 97.
[54] GDPR Art 83(4, 6).
[55] GDPR Art 21, Recital 70.
[56] Id. See Discussion supra Section 3.1(1)(iv).
[57] GDPR Recital 38.
[58] GDPR Art 6(1)(f).
[59] GDPR Recital 47.
[60] GDPR Art 88; Recitals 52, 127, 155.

workplace monitoring, and termination.[61] This competency must be balanced with the general principles of the GDPR.[62]

- **Sensitive Data in Business:** The GDPR heightens requirements for processing sensitive categories of data.[63] These categories significantly affect business operations, particularly in areas where profiling can influence socioeconomic decisions such as creditworthiness, insurance assessments, or other critical economic outcomes.

ii. Social

Profiling impacts social structures by influencing access to services, fairness in treatment, and the potential for discrimination:

- **Social Impacts of Profiling with Sensitive Data, Vulnerable Groups**: The GDPR underscores the heightened social risks associated with profiling based on sensitive data, such as racial or ethnic origin, religious beliefs, or health information, by generally prohibiting its processing.[64] Profiling in these contexts can perpetuate systemic discrimination, restrict access to essential services like healthcare or education, and deepen social inequalities, particularly for marginalized or vulnerable groups. These impacts highlight the critical importance of protective measures to ensure fairness, inclusion, and respect for fundamental rights in profiling practices. Given that profiling can perpetuate bias or amplify vulnerabilities, particularly for marginalized or vulnerable groups or children, the GDPR emphasizes protections against discrimination based on racial, ethnic, or socioeconomic factors, and stress minimizing harm in high-risk processing scenarios.[65]
- **Public Health and Social Research:** The GDPR enables the use of personal data for public health purposes.[66] Additionally, exceptions are carved out for public interest, as well as for scientific, historical, or statistical purposes.[67]

iii. Political

The GDPR addresses profiling in political activities, particularly concerning electoral processes and public security:

- **Sensitive Data and Political Profiling**: The GDPR categorizes data such as political opinions and religious or philosophical beliefs as special, granting them heightened protection.[68] These protections are particularly relevant in political contexts, where profiling based on such data could influence voter behavior and rights, electoral outcomes, or public opinion, necessitating robust safeguards to prevent misuse and ensure fairness.

---

[61] Id.
[62] GDPR Arts 5-11.
[63] GDPR Art 9.
[64] GDPR Art 9.
[65] GDPR Recitals 38, 75.
[66] GDPR Recitals 53, 54.
[67] GDPR Arts 89; 9(2)(h)-(j)
[68] GDPR Art 9.

- **Electoral Activities:** The GDPR acknowledges that political parties may process data on individuals' political opinions for democratic participation, providing an exception for these cases.[69] However, such profiling must include safeguards against misuse or manipulation, protecting the public interest.
- **Automated Decision-Making in Political Contexts:** The GDPR prohibits fully automated profiling that significantly impacts data subjects, inclusive of political rights.[70] For instance, this includes data processing and profiling that influences voting behavior, or restricts individuals from voting.
- **Freedom of Expression and Information**: The GDPR ensures that Member States balance the right to data protection with the right to freedom of expression and information, particularly in contexts like journalism, academia, and artistic or literary expression.[71] This balance is crucial for democratic values and applies broadly to contexts like audiovisual production, news archives, and press libraries, emphasizing a broad interpretation of freedom of expression to uphold its importance in democratic societies.[72]

3.2 Artificial Intelligence Act

The **EU Artificial Intelligence Act (AI Act)** is a cornerstone regulation aimed at ensuring the safe, transparent, and trustworthy development and deployment of AI systems within the European Union. Its overarching purpose is to mitigate risks posed by AI technologies while fostering innovation and safeguarding fundamental rights, such as privacy, fairness, and non-discrimination.

The AI Act does not focus exclusively on profiling but addresses it in practice as part of its broader mandate to regulate high-risk and prohibited AI applications.

The AI Act employs a **tiered risk-based approach** to regulate AI systems, assigning categories that dictate compliance requirements or outright bans: The higher the risk, the more potential for ban or elevated compliance requirements. **High-risk AI systems**, such as those used in law enforcement, creditworthiness assessments, or employment processes, are subject to stringent requirements, including risk assessments, transparency measures, and human oversight. At the highest level of restriction, **unacceptable-risk AI systems**, such as those involving manipulation, exploitation of vulnerable populations, or social scoring, are prohibited outright. These categories ensure that AI systems, including those engaging in profiling, align with fundamental rights and ethical standards.

By targeting the contexts and potential harms of AI-driven profiling, the AI Act integrates profiling into its broader goal of making AI systems accountable, transparent, and aligned with the values provided for by European regulatory frameworks.

---

[69] GDPR Recital 56.
[70] GDPR Art 22, Recital 71.
[71] GDPR Art 85, Recital 153.
[72] Id.

(1) Defining Features & Characteristics

This subsection will provide an overview of how the EU AI Act addresses profiling within its broader regulatory framework for artificial intelligence. It focuses on three key aspects: (i) definition and context, (ii) high-risk AI systems, and (iii) prohibited AI systems.
In summary to the below:

1. **Definition and Context**: The EU AI Act relies on definitions established in complementary legislation, particularly the GDPR, and addresses profiling indirectly as part of its broader mandate to ensure AI safety and ethical use.
2. **High-Risk AI Systems**: Profiling in high-risk systems is central to the Act's compliance framework, with stringent requirements for transparency, human oversight, and conformity assessments.
3. **Prohibited AI Systems**: The Act bans profiling in unacceptable-risk systems, such as those involving manipulation, exploitation, or social scoring, safeguarding fundamental rights and ethical principles.

These elements establish the foundation for understanding the role of profiling in the EU AI Act. Further exploration of each item is presented below.

i. Definition and Context

The EU Artificial Intelligence Act (AI Act) incorporates profiling as a critical activity within its regulatory framework, though it does not explicitly define the term. Instead, it relies on the **GDPR's definition of profiling**,[73] as the automated processing of personal data to evaluate, predict, or infer characteristics, behavior, or preferences of individuals. Profiling activities under the AI Act are typically associated with systems that infer sensitive data, evaluate personal attributes, or predict behavior, though with the added context of AI-processing, aligning them with GDPR protections and other EU legislation governing data use and privacy.

Profiling and Its Broader Legal Context, Data Management: The AI Act is a piece within the universe of laws that govern profiling in the EU, relying heavily on the GDPR for many of its profiling-specific governance, but enhancing protections around AI systems. Profiling activities within the AI Act typically involve systems that analyze personal data, structure it, and make predictions or evaluations about individuals. This includes applications in domains such as credit scoring, hiring, and law enforcement.[74] The AI Act aligns with existing EU legislation, particularly the GDPR, to ensure that AI-driven profiling adheres to principles of data protection, transparency, and accountability: The AI Act underscores that it does not replace existing Union laws governing personal data, but complements them to address the unique challenges posed by AI systems.[75]

The AI Act intertwines its AI compliance obligations with data management in the context of profiling systems. It acknowledges the importance of safeguarding personal data, establishing

[73] AI Act Art 3(52); GDPR Art 4.
[74] AI Act Annex III.
[75] AI Act Art 10.

that AI-profiling process must apply the principles of data minimization and data protection by design and by default, as required under Union data protection law.[76]

ii. High-Risk AI Systems

The EU AI Act establishes a governance structure for high-risk AI systems that directly affects profiling processes. This section outlines three critical dimensions of high-risk AI governance: (i) the criteria for classifying an AI system as high-risk, (ii) the compliance obligations these systems must meet, and (iii) the specific profiling-related applications subject to these heightened requirements.

(i) What Constitutes a High-Risk AI System?

-*Impact*: An AI system is classified as high-risk if it meets specific criteria under the EU AI Act. These systems are defined by their potential to significantly impact individuals' health, safety, or fundamental rights.[77]

-*Sector-specific*: The EU AI Act provides a categorization listing of sectors in which AI deployment is considered high risk. of Systems that are categorized as always considered high-risk include AI profiling processes deployed in sectors such as employment, education, law enforcement, access to essential services, and biometric identification.[78] Profiling activities, particularly when they materially influence decision-making or individual rights, are explicitly included.

-*Exceptions, and profiling*: Notably, an AI system classified high-risk such may avoid classification if it does not pose significant risks to health, safety, or rights, provided it performs limited or preparatory functions without materially influencing outcomes.[79] However, systems engaging in profiling are invariably high-risk.[80]

(ii) Compliance Requirements for High-Risk AI Systems

High-risk AI systems are subject to rigorous regulatory obligations before deployment to mitigate risks and uphold fundamental rights.[81] Key requirements include:

1. **Risk Management Systems, Assessment and Mitigation:** Providers must establish and maintain a risk management system throughout the system's lifecycle. This involves identifying, evaluating, and mitigating foreseeable risks, with particular focus on safeguarding vulnerable groups.
2. **High-Quality Datasets:** Systems must be trained, validated, and tested with datasets that are accurate, representative, and free of biases. Robust data governance practices, such

[76] AI Act Recital 69.
[77] AI Act Art 6, Recital 53.
[78] AI Act Art 6, Annex III.
[79] AI Act Art 6(3).
[80] Id.
[81] AI Act Chapter III Section 2; Chapter IX; European Commission. "Europe's approach to Artificial Intelligence." Shaping Europe's Digital Future, European Commission, https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai. Accessed 7 March 2025.

as pseudonymization and secure data handling, are mandatory to minimize risks and discriminatory outcomes.

3. **Documentation, Activity Logging and Traceability:** Systems must automatically log relevant events to enable post-market monitoring and ensure transparency in their operation.
4. **Detailed Documentation:** Providers must produce comprehensive technical documentation detailing the system's purpose, design, and compliance measures, allowing authorities to evaluate conformity.
5. **Human Oversight:** Deployers must retain meaningful human control over AI outputs. This includes the ability to interpret results, override system decisions, and halt operations when necessary to minimize risks.
6. **Transparency and Information Provision:** High-risk systems must include clear instructions for use, detailing their capabilities, limitations, and potential risks to ensure proper deployment and understanding by users.
7. **Robustness, Security, and Accuracy:** Systems must be designed to achieve high levels of reliability and resilience against errors, biases, or adversarial attacks, ensuring consistent performance in real-world scenarios.

(iii) High Risk Systems

The EU AI Act classifies certain AI applications as high-risk due to their potential to significantly affect individuals' rights, safety, and access to critical opportunities. Among these, systems involving profiling are prominently regulated, as their deployment often intersects with sensitive personal data, significant power imbalances, and fundamental rights. Below is an account of high-risk systems where profiling plays a critical role:

Biometrics: [82] Biometric profiling systems are tightly regulated due to their sensitivity and potential for misuse. These systems are prohibited or heavily restricted, particularly in publicly accessible spaces, unless narrowly justified for critical purposes, such as locating missing persons or preventing imminent threats.[83] High-risk applications include:

- **Remote Biometric Identification**: Identifying individuals in real-time in public spaces, often subject to strict legal oversight.
- **Biometric Categorization**: Grouping individuals based on inferred sensitive attributes, such as race or gender.
- **Emotion Recognition**: Profiling individuals by analyzing their emotional states, which raises ethical and privacy concerns.

Education: [84] In education and vocational training, high-risk AI systems influence significant decisions about individuals' opportunities and trajectories, directly affects fairness, equality, and access to education:

- Admission processes, where profiling determines access to institutions or programs.

[82] EU AI Act Annex III, 1.
[83] EU AI Act Recitals 3, 15-18, 32-39, 44, 54, 94-95; Art 5(1)(g), (2-7).
[84] EU AI Act Annex III, 3.

- Learning evaluations and assessments, where AI evaluates outcomes and personalizes educational paths.
- Behavior monitoring, such as detecting prohibited conduct during examinations.

Employment:[85] Employment-related AI systems often rely on profiling for critical decisions which have profound implications for workers' privacy, autonomy, and career outcomes, including:

- Recruitment and selection or candidate evaluation, where applications are filtered and ranked, inclusive of job advertisements.
- Performance monitoring and task allocation based on individual traits or behavior.
- Workplace relationship determinations, including promotion, termination, and other work-related decisions.

Essential Services: [86] Profiling in the context of access to essential public and private services can activate biases in these systems, with the risk of depriving individuals of critical resources or fair treatment, including:

- Evaluating eligibility for public benefits, such as healthcare or social assistance.
- Credit scoring and financial risk assessments, inclusive of assessment and pricing for life or health insurance.
- Emergency response systems, where profiling can prioritize or deprioritize resources.

Law Enforcement:[87] AI systems used in law enforcement are classified as high-risk due to their potential to impact fundamental rights, fairness, and procedural justice. These systems carry significant risks, including discrimination, errors, and misuse. High-risk categorization includes:

- Predicting the likelihood of individuals becoming victims of criminal offenses.
- Assessing evidence reliability during investigations or prosecutions.
- Forecasting the risk of offending or re-offending, factoring in personality traits, criminal history, or group behaviors.
- Profiling individuals to aid in detection, investigation, or prosecution of crimes, requiring strict safeguards to prevent misuse.

Migration: [88] AI systems in migration, asylum, and border control management involve profiling to:

- Assess risks, such as security or health, posed by individuals entering the EU.
- Evaluate applications for visas or asylum, including determining eligibility and evidence reliability assessments.
- Detect or identify individuals crossing borders, often using biometric profiling.

[85] EU AI Act Annex III, 4.
[86] EU AI Act Annex III, 5.
[87] EU AI Act Annex III, 6; Recital 59.
[88] EU AI Act Annex III, 7.

Justice Administration, Democratic Processes:[89] Profiling's impact on democracy is profound risks undermining democratic fairness and transparency. It can amplify biases, manipulate voter behavior, and compromise the integrity of key legal and democratic functions, including:

- Judicial processes, where AI assists in interpreting facts or laws.
- Elections, where profiling can influence voter behavior or electoral outcomes.

iii. ***Prohibitions and Unacceptable Risks***

The EU AI Act sets strict prohibitions on AI systems deemed to pose unacceptable risks, including profiling applications that can harm individuals or undermine fundamental rights. These prohibitions address activities where profiling leads to exploitation, discrimination, or significant harm. Below is an account of key prohibited uses of AI systems involving profiling.

Manipulation or Deception:[90] The AI Act strictly prohibits the use of AI systems that employ subliminal or purposefully **manipulative techniques designed to distort individuals' behavior**. These systems, by operating beyond a person's conscious awareness or employing deceptive strategies, impair individuals' ability to make informed decisions. Specifically, such systems are banned when they:

- Materially distort behavior, leading individuals or groups to decisions they would not have otherwise made.
- Cause or are likely to cause significant harm to individuals, groups, or other affected parties.

Exploitation of Vulnerability:[91] The AI Act prohibits systems that exploit vulnerabilities related to an individual's **age, disability, or socio-economic status**, causing or likely to cause significant harm.

Evaluation or Classification for Social Scoring: [92] Social scoring systems are banned when they classify or evaluate individuals based on inferred personal or behavioral characteristics in ways that:

- Lead to **unfavorable treatment** in contexts unrelated to the original purpose of data collection.
- Result in **disproportionate or unjustified impacts** based on social behavior or inferred traits.

Criminal Profiling:[93] AI systems that perform **criminal risk assessments** solely based on profiling or inferred personality traits are prohibited. However, exceptions exist for systems that support **human oversight** with evidence-based assessments linked to criminal activities.

---

[89] EU AI Act Annex III, 8.
[90] EU AI Act Art 5(1)(a).
[91] EU AI Act Art 5(1)(b).
[92] EU AI Act Art 5(1)(c).
[93] EU AI Act Art 5(1)(d).

Surveillance and Facial Recognition:[94] AI systems that create or expand **facial recognition databases** using untargeted scraping of online images or CCTV footage are banned. Additionally, the **real-time use of remote biometric identification** in public spaces by law enforcement is prohibited unless:

- Necessary to locate missing persons or victims of crimes like trafficking.
- Aimed at preventing imminent threats, such as terrorist attacks.
- Directed at identifying suspects in severe criminal investigations.

Even in these cases, stringent conditions apply, including judicial authorization and geographic, temporal, and database constraints.

Emotional Inference in Workplace or Education:[95] AI systems that profile individuals by inferring emotions in **workplace or educational settings** are prohibited, except where explicitly designed for **medical or safety purposes**.

Biometric Categorization:[96] The use of biometric data for categorizing individuals by **sensitive attributes**, such as race, religion, or political beliefs, is prohibited. However, exceptions apply to law enforcement for lawful biometric dataset management.

(2) Sectorial Classification

Profiling under the AI Act is regulated to address the risks associated with AI-driven decision-making and to safeguard fundamental rights. The Act adopts a tiered risk-based framework, targeting high-risk and prohibited systems, with a strong emphasis on transparency, accountability, and human oversight. Its provisions extend to a broad range of applications, from biometric identification to law enforcement and democratic processes, protecting AI-driven profiling in diverse contexts.

i. Business

The AI Act addresses profiling in business contexts by regulating high-risk and prohibited applications that influence economic outcomes, workplace dynamics, and consumer interactions:

- **Employment Profiling (High-Risk or Prohibited):** Profiling systems used in employment processes, such as recruitment, performance monitoring, and workforce management, are classified as high-risk. These systems influence critical decisions, including promotions and terminations, which can have significant consequences for individuals' careers.
- **Consumer Credit and Insurance (High-Risk):** Profiling-based AI systems in finance and insurance evaluate creditworthiness, assess risk for life and health insurance, and determine eligibility for essential services. These systems are inherently high-risk due to their potential to deny individuals fair access to loans, insurance coverage, or other financial opportunities.

[94] EU AI Act Art 5(1)(e, f, g, h).
[95] EU AI Act Art 5(1)(f).
[96] EU AI Act Art 5(1)(g-h); 5(2) et seq.

- **Biometric Applications in Commerce (High-Risk or Prohibited):** Businesses deploying biometric profiling systems, such as emotion recognition for consumer analytics or categorization based on sensitive traits like race or gender, face stringent regulations. The AI Act prohibits systems that exploit biometric data for discriminatory purposes or emotional inference in sensitive contexts like workplaces and education, ensuring that commercial uses do not infringe on personal dignity or equality.

ii. Social

Profiling has extensive social implications, affecting access to critical services, equality in education, and the rights of vulnerable populations:

- **Access to Essential Services (High-Risk):** Profiling systems used to evaluate eligibility for healthcare, social benefits, and emergency services are considered high-risk due to their direct impact on individuals' well-being. For example, errors in these systems could unfairly deny individuals access to life-saving treatments or public assistance.
- **Education and Equality (High-Risk):** AI-driven profiling in education and vocational training determines admissions, evaluates learning outcomes, and monitors behavior during assessments. Such applications are classified as high-risk because they directly influence individuals' opportunities and trajectories.
- **Migration and Border Control (High-Risk):** Profiling systems in migration and asylum processes assess security risks, evaluate eligibility for visas or asylum, and identify individuals at borders. These high-risk applications have life-altering consequences, especially for vulnerable populations.
- **Criminal Profiling (High-Risk or Prohibited)**: Criminal profiling systems are classified as high-risk due to their significant impact on fundamental rights, fairness, and procedural justice. predicting the likelihood of individuals becoming victims of crime, assessing evidence reliability, and forecasting the risk of offending or reoffending based on factors like personality traits, criminal history, or group behaviors. Profiling systems that solely rely on automated assessments of traits to predict criminal behavior are prohibited.

iii. Political

The AI Act recognizes the significant influence profiling can have on democratic processes, law enforcement, and governance, regulating high-risk and prohibited uses accordingly:

- **Democratic Integrity (High-Risk):** Profiling in electoral processes, such as targeting voters or influencing voting behavior, is tightly regulated as high-risk. These applications must comply with the AI Act's transparency and accountability requirements to preserve democratic fairness and prevent manipulation.
- **Justice and Law Enforcement (High-Risk or Prohibited):** AI, as deployed in judicial decision-making, is considered high-risk. Profiling systems used in law enforcement to assess criminal risk, predict behavior, and support investigations are classified as high-risk, with certain biometric data or criminal history features being prohibited.
- **Social Scoring (Prohibited):** Profiling systems used for social scoring are explicitly banned under the AI Act. Such systems, which evaluate or classify individuals based on

inferred traits or behaviors, are prohibited when they result in unjustified or disproportionate treatment or embed biases that undermine fairness and equality.

3.3 Digital Services Act Package: Digital Services Act & Digital Markets Act

The **Digital Services Act (DSA)** and the **Digital Markets Act (DMA)** establish a unified regulatory framework across the EU to govern digitally-powered commercial interactions. Together, they set out **obligations for digital platforms**, balancing fundamental rights protection with economic growth.

At their core, the **DSA** focuses on the **responsibilities of online intermediaries and platforms**, including social networks, marketplaces, and search engines—especially those with **over 45 million users**, which face the strictest requirements. Meanwhile, the **DMA** targets **"gatekeeper" platforms**—dominant digital players that control access to key online services—to prevent **anti-competitive practices** and ensure a more open digital market. Though they both overlap in the safety of the markets and commercial interactions, generally the two laws can be characterized for their focus:

- *Business to Consumer*: **The DSA** primarily governs **B2C interactions**, focusing on how digital platforms engage with consumers, including content moderation, recommender systems, targeted advertising, and systemic risks like misinformation and online harms. It ensures that profiling and data-driven personalization do not undermine consumer rights, transparency, or fundamental freedoms.
- *Business to Business*: **The DMA** is more focused on **B2B data markets**, regulating how **gatekeepers** control access to digital markets, manage business users' data, and prevent anti-competitive behavior. It seeks to ensure that dominant platforms do not unfairly leverage their data advantages to restrict competition or impose unfair terms on businesses relying on their core platform services.

Digital Services Act (DSA) Summary

The DSA establishes a regulatory framework for **online intermediaries and platforms**, including marketplaces, social networks, and app stores. Its primary aim is to **prevent illegal and harmful activities online**, combat disinformation, and ensure user safety and fundamental rights**.**

Key Goals of the DSA:

- **Strengthen online safety and consumer protection** by requiring platforms to remove illegal content, improve seller traceability, and implement stricter safeguards against scams and harmful activities.
- **Increase transparency and accountability** through new rules on content moderation, algorithmic recommendations, and online advertising, including bans on targeted ads based on sensitive data and protections, and measures to counter disinformation, election manipulation, and other systemic risks. These platforms must also ensure crisis response mechanisms during public health and security emergencies.

- **Impose stricter obligations on very large online platforms (VLOPs) and search (VLOSEs) engines** by requiring them to assess and mitigate systemic risks, undergo independent audits for risk assessment and mitigation measures, enhance transparency in algorithmic recommendations, and prevent the abuse of their services, ensuring accountability for platforms with over 45 million users in the EU.

DIGITAL MARKETS ACT (DMA) SUMMARY

The DMA aims to create a **fairer and more competitive digital market** by regulating the power of large digital platforms acting as **gatekeepers**. These gatekeepers, which include search engines, app stores, and messaging services, play a crucial role in the digital ecosystem and must comply with specific obligations and restrictions to ensure fair competition.

Key Aspects of the DMA:

- **Defines "gatekeepers"** and targets entry into the digital marketplace.
- **Imposes obligations and restrictions** to prevent unfair business practices.
- **Works alongside EU competition law**, complementing existing regulations without replacing them.

(1) Defining Features & Characteristics

i. Definition and Context

The **DSA** and **DMA** do not directly regulate profiling as their primary focus. However, they impose obligations on platforms and gatekeepers that influence the use of profiling. These measures are intended to limit the exploitative use of profiling in digital markets and reinforce consumer choice.

- The **DSA** establishes obligations for online platforms, search engines, and digital services to combat illegal content, misinformation, and harm while ensuring transparency and accountability. This includes their data management and profiling capabilities to influence digital services. It imposes stricter transparency requirements on targeted advertising and recommender systems, mandates user control over personalization settings, and requires that certain algorithmic responses are not based on profiling.
- The **DMA** governs gatekeepers—large digital platforms that control access to markets—by enforcing rules on fair competition, interoperability, and user interactions. It restricts gatekeepers from using non-public business user data for competitive advantage, mandates transparency in advertising and recommender systems, and enhances user control over data used for profiling.

Both the **DSA**[97] and the **DMA**[98] refer to the profiling definition provided in the **General Data Protection Regulation (GDPR)** by incorporation.

The following are specific features addressing profiling in key areas, introduced by each of the Acts:

ii. Transparency in Profiling

DSA: *Requires transparency in recommendation algorithms*.[99] Online platforms using recommender systems must disclose their main parameters in their terms and conditions. If these involve profiling of users through any data management processes, these must be disclosed. Users must be able to understand why specific content is recommended, including: (i) Key criteria influencing recommendations, and (ii) the significance and impact of those criteria.

DMA: *Emphasizes the need for clear and accessible information*[100] on profiling practices used by gatekeepers. To enhance transparency:

- Data Utilization & Processing: Gatekeepers must **explain how profiling works**, including whether personal data is used and for what purpose. Users should be informed about the **processing methods, duration, and impact** of profiling on services.
- Fairness & Competition: Transparency and restrictions on profiling prevent **deep consumer profiling from becoming the industry standard**. Without such measures, only dominant gatekeepers can accumulate and exploit large-scale user data, leaving **SMEs unable to compete**. Clear rules allow **privacy-conscious and smaller competitors** to offer alternative models.
- Institutional Involvement: The **European Data Protection Board (EDPB)** oversees compliance to ensure alignment with GDPR.

iii. Advertising and Profiling Restrictions

DSA: *Prohibits targeted ads based on profiling*[101] that use **special categories of personal data** (e.g., race, religion, health data) as defined in GDPR Article 9(1).

DMA: *Prohibits gatekeepers from processing personal data*[102] of end-users across third-party services for targeted advertising unless users have given explicit consent.

---

[97] Regulation 2022/2065, of the European Parliament and of the Council, on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act), 2022 O.J. (L 277) 1 ("DSA") at Arts 26.3, 28.2, 38; Recital 69.

[98] Regulation 2022/1925, of the European Parliament and of the Council, on Contestable and Fair Markets in the Digital Sector and Amending Directives 2019/1937 and 2020/1828 (Digital Markets Act), 2022 O.J. (L 265) 1 at Art 2.31; Recital 72.

[99] DSA Art 27.

[100] DMA Recital 72.

[101] DSA Art 26.3.

[102] DMA Art 5.2(a).

iv. Protection of Minors

DSA: *Platforms cannot present profiling-based advertisements to minors*[103] when they are reasonably certain that the recipient is underage.

DMA: *Recognizes children as a vulnerable group requiring special protectio*[104] highlighting that commercial communications and creating user profiles should be restricted.

v. Non-Profiling Recommendation Systems

DSA: *Requires VLOPs and VLOSEs to provide at least one recommender system that does **not** rely on profiling*.[105]

vi. Audit of Profiling Techniques

The DSA and DMA impose strict auditing and oversight requirements on major digital platforms to ensure transparency and accountability in their profiling practices. These audits assess how profiling influences content delivery, advertising, and user interactions, with regulatory bodies overseeing compliance to safeguard consumer rights and market fairness.

- Obligation to Audit: Both the DSA[106] and DMA[107] require major digital platforms to conduct independent audits assessing their compliance with transparency, risk management, and accountability obligations. **Per the DSA**, VLOPs, VLOSEs, and gatekeepers must provide detailed assessments of how profiling is used in recommender systems, targeted advertising, and other core platform services. This audit must evaluate how profiling techniques are applied, their impact on users, and whether platforms implement adequate mitigation measures to ensure compliance. **Per the DMA**, gatekeepers must submit a formal audit of their consumer profiling techniques within six months of designation, with annual updates to ensure continued compliance.
- Public & Regulatory Oversight: Both frameworks mandate public disclosure and regulatory supervision of profiling practices. Platforms must document and publicly report how profiling influences content visibility, advertising, and user engagement. The **European Board for Digital Services** (EBDS)[108] oversees DSA audits, ensuring compliance with GDPR and fundamental rights protections, while the **European Data Protection Board** (EDPB)[109] monitors DMA audits to enforce data protection standards. A public summary of gatekeeper profiling audits must be made available under the DMA, striking a balance between transparency and business confidentiality.

[103] DSA Art 28.2.
[104] DMA Recital 38.
[105] DSA Art 38.
[106] DSA Arts 37, 61, 42.4, 63.1(b); Recitals 92, 93, 143.
[107] DMA Art 15.
[108] DSA Section 3; Recitals 91, 131.
[109] DMA Art 15; Recital 72.

vii. Dark Patterns

The **DSA** addresses **dark patterns**,[110] which are deceptive or manipulative design practices that impair users' ability to make **autonomous and informed decisions**. Example of these behaviors include:

- **Manipulative Interface Design:** Structuring choices in a non-neutral manner (e.g., visually prioritizing certain options to benefit the platform).
- **Exploitative Nudging:** Repeatedly requesting decisions that users have already made or making cancellations more difficult than sign-ups.
- **Default Bias:** Using pre-set options that are hard to change, leading to biased decision-making.
- **Obstructive Practices:** Making it unreasonably difficult to discontinue purchases or log out.

viii. Electoral Processes

Political Participation & Repositories: Advertising systems on VLOPs and VLOSEs present risks to electoral processes due to their ability to target users based on behavior within and outside the platform. To safeguard election integrity, these platforms must provide public access to **advertisement repositories**, detailing ad content, advertisers, and targeting criteria. This transparency helps mitigate risks such as political disinformation, manipulative campaign techniques, and covert influence operations, ensuring fair political participation and protecting democratic processes.[111]

March 26, 2024 Guidelines:[112] The European Commission issued DSA-related guidelines to **mitigate systemic online risks** during elections. **VLOPs and VLOSEs must:**

1. Strengthen internal processes to analyze electoral risks.
2. Implement election-specific mitigation measures (e.g., promoting official election information, media literacy, and reducing misinformation).
3. Address risks linked to **AI-generated content** (e.g., deepfakes, synthetic media).
4. Cooperate with authorities, independent experts, and civil society to prevent **foreign interference, disinformation, and cybersecurity threats**.
5. Conduct **post-election reviews** of risk mitigation strategies and publicly disclose findings.

These guidelines aim to preserve election integrity, reduce disinformation, and prevent the misuse of profiling-based targeting during electoral campaigns.

ix. Summary: Very Large Online Platforms & Search Engines; Gatekeepers

DSA: *Very Large Online Platforms & Search Engines*[113]

---

[110] DSA Recital 67.

[111] DSA Recital 95.

[112] European Commission, Guidelines for Providers of VLOPs and VLOSEs on the Mitigation of Systemic Risks for Electoral Processes, 2024 O.J. (C 3014) 1; European Commission Press Release IP/24/1707, Commission Publishes Guidelines Under the DSA for the Mitigation of Systemic Risks Online for Elections (Mar. 26, 2024).

[113] DSA Sections 5, Recitals 47-49, 75-105, 137-142.

Definition: Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs) are digital services with over **45 million** monthly users in the EU. Due to their scale and impact, they are subject to stricter obligations under the DSA. Characteristics on the process of designation include the following:

- Platforms and search engines must publish their user numbers every six months.
- If a service exceeds 45 million users, the European Commission designates it as a VLOP or VLOSE (a service can lose its designation if user numbers fall below 45 million for one year).

Special Obligations for VLOPs and VLOSEs:
Once designated, VLOPs and VLOSEs must implement **risk mitigation measures**, comply with **transparency requirements** and **crisis response protocols**, and undergo **external audits**. These requirements go beyond those for smaller platforms.

- **Systemic Risk Assessments**: VLOPs and VLOSEs must identify, analyze, and mitigate risks related to:
  - Illegal content (e.g., hate speech, counterfeit goods).
  - Fundamental rights violations (e.g., privacy, freedom of expression, child protection).
  - Electoral manipulation and public security threats (e.g., disinformation, AI-generated deepfakes).
  - Public health risks (e.g., misleading medical information).
- **Crisis response protocols**: During a "crisis event" (i.e. serious threat to public security or health) the Commission may take strictly necessary, justified and proportionate actions to ensure VLOPs and VLOSEs do not contribute to the determined threat.
- **Mandatory Transparency Measures**:
  - *Algorithmic Accountability*: Platforms must disclose how their algorithms influence content visibility and ensure recommender systems offer at least one option not based on profiling.
  - *Ad Repository*: They must publish all advertisements, including who paid for them and how they were targeted.
  - *Data Sharing for Research*: Vetted researchers must be granted access to platform data to analyze systemic risks.
- **Compliance & Audits**:
  - *Internal Compliance Function*: VLOPs and VLOSEs must create a dedicated compliance function independent of operational management.
  - *Annual Independent Audits*: These audits assess compliance with the DSA and ensure platforms are effectively mitigating risks.
  - *Data Access for Authorities*: Platforms must grant EU regulators and vetted researchers access to platform data for oversight purposes.

DMA: *Gatekeepers*[114]

Gatekeeper definition:

Gatekeepers, as are large digital platforms that provide core platform services such as online search engines, app stores, and messaging services. A company is designated as a gatekeeper under a set of circumstances:

- **Significant impact**: Has significant influence on the EU internal market, with a strong economic position across EU countries.
- **Intermediation with power**: Controls a core platform service that serves as a key gateway between businesses and end users, linking a large user base to businesses.
- **Entrenchment**: Holds an entrenched and durable market position or is expected to in the near future.

Current gatekeepers: The European Commission has designated seven companies, for a total of 24 core platform services, as gatekeepers: Alphabet, Amazon, Apple, ByteDance, Meta, Microsoft, and Booking.com.[115]

Gatekeeper Obligations Under the DMA:

The DMA imposes additional obligations on gatekeepers to ensure fair competition and transparency, defining what they must do and cannot do in their operations:[116]

- **Core active obligations for gatekeepers:**
  - *Interoperability*: Allow third parties to interoperate with their services under specific conditions.
  - *Data Access*: Let business users access their own generated data from the gatekeeper's platform.
  - *Advertising Transparency*: Provide advertisers with the tools needed for independent ad verification.
  - *Business Freedom*: Allow companies using their platform to promote and conclude contracts outside the gatekeeper's ecosystem.
- **Negative obligations for gatekeepers:**
  - *Self-Preferencing*: Gatekeepers cannot favor their own products/services over competitors on their platforms.
  - *Restricting Business Links*: They cannot prevent consumers from linking to businesses outside their ecosystem.
  - *Forcing Pre-Installed Apps*: Users must be allowed to uninstall pre-installed software if they wish.

---

[114] DMA Recitals 3-8, 29-37, 43-46; DMA Arts 2.1, 3; European Commission, Digital Markets Act (DMA) Overview, EUR-Lex, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en (last visited Feb. 14, 2025).

[115] European Commission, Gatekeepers Under the Digital Markets Act, European Commission, https://digital-markets-act.ec.europa.eu/gatekeepers_en (last visited Feb. 14, 2025).

[116] DMA Chapter III; European Commission, Commission Designates First Gatekeepers Under the Digital Markets Act, European Commission Press Corner, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4328 (last visited Feb. 14, 2025); European Commission, Digital Markets Act (DMA) Overview, European Commission, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en (last visited Feb. 14, 2025).

- *Cross-Platform Tracking Without Consent*: Gatekeepers cannot track users across different services for targeted ads without explicit consent.

(2) Sectorial Classification

Profiling under the **DSA** and **DMA** is structured to address risks associated with digital platforms and gatekeepers while ensuring fair competition and user protection. These acts introduce obligations that affect how platforms manage data, algorithmic decision-making, and user interactions, aiming to balance fundamental rights with economic growth.

i. Business

The DSA and DMA regulate profiling in business contexts by introducing obligations for platforms that influence market competition, digital advertising, and consumer interactions:

- **Content Recommendation & Algorithmic Transparency (DSA):** Online platforms that use recommender systems must disclose their main parameters, including how profiling influences the visibility of content, ads, and digital services. Also, platforms must provide recommendations that are not based on profiling.
- **Advertising & Targeting Restrictions (DSA & DMA):** The DSA prohibits targeted ads based on sensitive personal data; while the DMA restricts gatekeepers from processing user data for advertising unless explicit consent is given. This prevents dominant platforms from exploiting personal data for unfair competitive advantage.
- **Gatekeeper Obligations, Fair Competition, & Market Access (DMA):** Large platforms designated as gatekeepers must comply with obligations ensuring fair competition, including requirements for data transparency in profiling practices, and restrictions on anti-competitive data accumulation. The DMA ensures that large digital platforms do not create barriers to competition through excessive profiling practices, allowing SMEs and alternative services to compete.

ii. Social

Profiling impacts users; access to services, privacy rights, and the protection of vulnerable groups:

- **Protection of Minors (DSA & DMA):** The DSA establishes that platforms are prohibited from delivering profiling-based advertising to minors when reasonably certain of their age. The DMA also highlights children's special need for protection from commercial profiling.
- **Dark Patterns & Manipulative Design (DSA):** The DSA addresses deceptive interface designs (e.g., making cancellations harder than sign-ups, default bias, and misleading nudges), ensuring users maintain autonomy over their choices.
- **Audit & Compliance Requirements (DSA & DMA):** Platforms are subject to independent audits to assess profiling risks, algorithmic bias, and systemic impacts.

iii. Political

Profiling is regulated in political contexts to prevent undue influence, protect democratic processes, and ensure regulatory oversight:

- **March 26, 2024 Guidelines (DSA):** The European Commission issued DSA-related guidelines to mitigate systemic online risks during elections. VLOPs and search engines must:
    1. Strengthen internal processes to analyze electoral risks.
    2. Implement election-specific mitigation measures (e.g., promoting official election information, media literacy, and reducing misinformation).
    3. Address risks linked to AI-generated content (e.g., deepfakes, synthetic media).
    4. Cooperate with authorities, independent experts, and civil society to prevent foreign interference, disinformation, and cybersecurity threats.
    5. Conduct post-election reviews of risk mitigation strategies and publicly disclose findings.
- **Advertising & Transparency (DSA):** Advertising systems on VLOPs and VLOSEs present risks to electoral integrity due to their ability to target users based on behavior both within and outside platforms. To safeguard elections, these platforms must provide public access to advertisement repositories, detailing ad content, advertisers, and targeting criteria. Platforms must ensure that political ads are clearly labeled and that profiling-based targeting of political content adheres to transparency standards. This transparency mitigates risks such as political disinformation, manipulative campaign techniques, and covert influence operations, ensuring fair political participation and protecting democratic processes.

3.4 Right to Repair Directive

The **Right to Repair Directive**[117] establishes a legal framework to ensure that consumers can repair products rather than replace them, extending product lifecycles, reducing electronic and consumer waste, and promoting a circular economy. The Directive mandates that manufacturers provide repair services, spare parts, and repair-related information for goods that are subject to EU repairability requirements, ensuring that repair remains a viable and accessible option.

At its core, the Directive introduces a **legally enforceable obligation to repair**, standardizes transparency requirements for repair services, and creates an **EU-wide repair platform** to connect consumers with repair providers. Independent repairers are explicitly protected under the law, ensuring that manufacturers cannot impose unfair restrictions that would limit consumers' ability to seek third-party repair services.

While this Directive does not explicitly regulate profiling, its **digital components—such as the European Online Repair Platform and repair information forms—introduce data governance implications**. The way repair data is processed, categorized, and shared can influence consumer profiling, potentially shaping markets for repair services, insurance policies, and product lifespan assessments. These elements bring the Right to Repair Directive into conversation with broader EU data protection and digital regulations, ensuring that consumers

[117] Directive (EU) 2024/1799 of the European Parliament and of the Council of 13 June 2024 on common rules promoting the repair of goods and amending Regulation (EU) 2017/2394 and Directives (EU) 2019/771 and (EU) 2020/1828, 2024 O.J. (L 277) 1 ("Right to Repair Directive").

retain control over their repair-related data while benefiting from fair and accessible repair services.

(1) Defining Features & Characteristics

i. Definition and Context

The **Right to Repair Directive** formalizes repair obligations for manufacturers and enhances consumers' access to repair services across the EU. It directly supports the **EU Green Deal's**[118] sustainability goals by reducing premature product disposal and fostering a circular economy.

The Directive applies to goods that are subject to reparability requirements under EU law and ensures that repair services remain accessible.[119] It establishes **rules on repair transparency, access to spare parts, and consumer rights**, creating a standardized framework that manufacturers, repair service providers, and consumers must follow.

While not an AI, profiling, or data-driven regulation, the Directive intersects with data governance through its **online repair platform** and **required transparency measures**, which involve **the collection and processing of consumer and product-related data**.

ii. Obligation to Repair & Consumer Rights

The Directive mandates that manufacturers **must offer repair services for certain products**.[120] This provision aims to prevent planned obsolescence and ensures that consumers have a legally backed right to request repair. Key features include:

- Mandatory Repair Services: If a product is covered by EU reparability requirements, manufacturers must provide repair options at a reasonable price and within a reasonable timeframe.
- Communication of Repair Rights[121] & European Repair Information Form:[122] Manufacturers must clearly inform consumers of their repair obligations. A **European Repair Information Form** is established to ensure consumers receive key details about repair services before committing to a contract. The form, which must be provided on a durable medium and free of charge (except when a diagnostic service is required), includes essential information such as the repairer's identity, defect diagnosis, estimated price, repair duration, and available ancillary services. Once issued, its terms remain valid for 30 days, enhancing transparency and consumer confidence in repair transactions.

[118] Right to Repair Directive Recital 5.
[119] Right to Repair Directive Art 5.
[120] Id.
[121] Right to Repair Directive Art 6.
[122] Recitals 10-14, 23, 32.

iii. European Online Repair Platform & Data Governance

The **Directive establishes an EU-wide repair platform** to help consumers find repair providers, refurbished goods, and repair resources.[123] This platform introduces data-sharing and transparency obligations, which align with broader EU digital governance principles.

The platform must comply with EU data protection laws (GDPR, DSA), ensuring that consumer data is not exploited for commercial tracking or behavioral profiling**.**

Role of the EU and Member States:[124]

- The **European Commission** is responsible for developing and maintaining the platform's **common online interface,** ensuring it is accessible in all official EU languages and complies with **data protection laws**. The Commission also oversees the **technical operation** of the platform and manages user queries related to its functioning.
- **Member States** must either **establish national repair sections** within the European online platform that meet the Directive's requirements.

iv. Independent Repairers & Market Competition

The Directive **protects independent repairers** from unfair restrictions imposed by manufacturers.[125] Features of this mechanism include:

- No Discriminatory Practices: Manufacturers cannot refuse repair services because a product was previously repaired by an independent repairer.
- Access to Spare Parts: Manufacturers must provide spare parts, tools, and software access at a reasonable price, preventing anti-repair barriers.
- Ban on Repair-Blocking Tactics: The Directive prohibits hardware or software techniques that obstruct independent repairs, such as digital locks or contractual clauses.

(2) Sectoral Implications

i. Business

The Directive reshapes repair markets, establishing an ecosystem in which manufacturers compete with independent repairers and prioritize product longevity over replacement cycles.

- **New Market Standards & Expansion of the Circular Economy**: Manufacturers must invest in repair services and adapt business models that align with sustainable product lifecycles.
- **Impact on Digital Ecosystems & the Role of Nations and the EU**: Repair data could be analyzed by manufacturers, insurers, and third-party platforms to profile consumer repair habits, influencing warranty pricing and service availability. Essentially, this directive creates a new market for repair data, managed in its architecture by the EU and nation states, but in a much more disaggregated manner, through independent repair forces.

[123] Right to Repair Directive Art 7.
[124] Right to Repair Directive Art 5.6; Recitals 19, 23, 38
[125] Right to Repair Directive Art 7; Recitals 26-34.

ii. Social

The Directive enhances consumer rights by giving individuals more control over their product choices and repair options.

- **Strengthening Consumer Autonomy**: Consumers can repair instead of replace, reducing unnecessary spending.
- **Transparency & Accessibility**: The European Online Repair Platform democratizes repair service access, ensuring consumers are informed about repair options; alongside a unified repair form for the EU.
- **Data & Privacy Considerations**: The use of repair data must align with EU privacy standards, ensuring no commercial profiling based on repair behaviors. This takes place at the private commercial level, as well as in the governmental administrative realm (in reference to the European Online Repair Platform).

iii. Political

The Right to Repair Directive carries broader regulatory and policy implications with regards to standardization of repair data and public data governance, pertaining to interactions between EU and national governments.

- **Standardization of Repair Rights Across the EU:** By harmonizing repair laws, the Directive prevents regulatory fragmentation and strengthens the EU's single market for repair services.
- **Governmental Oversight & Public Sector Data Use:** The European Online Repair Platform introduces a government-managed digital infrastructure that requires public-sector oversight of repair markets, creating an intersection between consumer rights, industrial policy, and data governance.

3.5 Unfair Commercial Practices Directive

The **Unfair Commercial Practices Directive (UCPD)** establishes the legal framework for consumer protection against deceptive, aggressive, and unfair business practices within the EU. It aims to ensure fairness in business-to-consumer transactions by prohibiting practices that distort consumer decision-making, whether through misleading information, coercion, or exploitative marketing tactics.

At its core, the UCPD sets **general principles for fairness in commercial practices**, covering transparency in advertising, contract terms, and business conduct. It defines **unfairness** based on two key criteria: a practice must (1) violate professional diligence and (2) materially distort consumer behavior, particularly by impairing the consumer's ability to make an informed decision. The directive also includes **a blacklist of automatically prohibited practices**, such as false claims of limited stock, hidden costs, and high-pressure sales tactics.

While the UCPD does not explicitly regulate **profiling**, its provisions on misleading and aggressive commercial practices may apply to **AI-driven personalization, dark patterns, and manipulative advertising techniques**. As businesses increasingly use behavioral data to

influence purchasing decisions, the directive plays a growing role in addressing digital consumer risks.

Below is an analysis of how the UCPD relates to profiling, the challenges it addresses, and its effectiveness in the evolving digital economy:

(1) Defining Features & Characteristics

i. Definition and Context

The Unfair Commercial Practices Directive (UCPD) establishes a uniform framework for regulating **business-to-consumer commercial practices** across the EU, ensuring consumer protection from **misleading and aggressive commercial behavior**. However, the Directive does not specifically regulate profiling or data-driven consumer targeting. Instead, it focuses on prohibiting practices that distort consumer decision-making, particularly through deception, coercion, or undue influence.

While profiling can sometimes amplify misleading or aggressive commercial practices—such as hyper-personalized advertising that exploits consumer vulnerabilities—the UCPD **does not provide explicit rules on profiling itself**. Instead, it sets broad principles that could indirectly apply when profiling is used in a manner that misleads or pressures consumers into commercial transactions.

ii. Unfair Practices

The UCPD prohibits all unfair commercial practices. While **data-driven or AI targeting and profiling are not explicitly covered**, practices that **exploit consumer vulnerabilities through behavioral manipulation** could be scrutinized under these categories. Practices are unfair when they fulfill certain characteristics, including:

- Contrary to professional diligence: The practice disregards the standard of care in good faith reasonably expected to be exercise towards customers in a field of activity.[126]
- Material distortion of economic behavior: A practice that alters or is likely to alter the economic behavior of the average consumer. If the practice targets a vulnerable consumer group, its impact is assessed from the perspective of the average member of that group. "Materially distorting consumer behavior" means interfering with a consumer's ability to make an informed choice, leading them to a transactional decision they otherwise wouldn't have made.[127]

Commercial practices that are categorized as unfair include:

[126] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC, and 2002/65/EC of the European Parliament and of the Council, and Regulation (EC) No 2006/2004 of the European Parliament and of the Council, 2005 O.J. (L 149) 22 ("UCPD") at Arts 5.2(a), 2(h); Recital 20.

[127] UCPD Arts 5.2(b), 5.3, 2(e).

- **Misleading Practices**:[128] A commercial practice is misleading when (i) it presents false, ambiguous, or deceptive information, or (ii) it omits or withholds essential details. This must be done in a way that prevents consumers from making informed decisions. Even if factually correct, information can still be misleading if its overall presentation deceives or is likely to deceive the average consumer, ultimately influencing them to make a transactional decision they wouldn't have otherwise taken. A practice is also considered misleading if it provides key information in an unclear, unintelligible, ambiguous, or untimely manner, or if it conceals its commercial intent.
- **Aggressive Practices**: [129] A practice is aggressive when businesses use harassment, coercion, or undue influence to pressure consumers into purchases. These tactics impair a consumer's ability to make free and informed decisions. Key factors in determining aggressiveness include timing, location, nature, persistence, threats (inclusive of any actions that cannot legally be taken), exploitation of conditions in the buyer to unduly influence buying behavior.
- **Practices which are always considered unfair ('blacklisted')**: [130] A set of automatically prohibited practices is provided by the UCPD. While misleading or aggressive practices are subject to demonstrability that they are causing a consumer to make a commercial decision they would not otherwise, these practices are determined to be automatically unfair. These include material misrepresentations of commercial interactions and products, but are not directly related to profiling or AI.

(2) Sectoral Implications[131]

i. Business

The UCPD indirectly regulates profiling by imposing strict rules on how businesses can market and advertise products, limiting the use of manipulative or misleading profiling-based strategies:

- **Deception, Aggression**: Businesses must ensure that AI-driven advertising and profiling-based marketing do not deceive or manipulate consumers. If profiling-based AI systems generate misleading or coercive commercial messages, businesses remain responsible under the UCPD.
- **Limitations on Hyper-Personalization**: The UCPD restricts businesses from using profiling to create artificial urgency, scarcity, or psychological pressure that distorts consumer choices.

ii. Social

The UCPD does not explicitly focus on social implications, but its regulation of unfair commercial practices has indirect effects on consumer autonomy and trust in digital markets. By restricting deceptive and manipulative profiling-based advertising, the Directive helps prevent

[128] UCPD Arts 6, 7.
[129] UCPD Arts 8, 9.
[130] UCPD Art 5.5, Annex I; Commission Staff Working Document, Fitness Check of EU Consumer Law on Digital Fairness, SWD (2024) 230 final (Oct. 3, 2024) ("Fitness Check") at 3.
[131] NTD: To finalize

consumer exploitation, particularly for vulnerable groups. However, its primary focus remains on commercial fairness rather than broader societal outcomes.

iii. Political

The UCPD primarily serves as a consumer protection framework, harmonizing unfair commercial practice rules across EU Member States. While it does not directly engage in political regulation, it ensures a common standard for addressing manipulative business practices, including those involving profiling-based marketing.

3.6 DATA ACT

The **Data Act** is a key regulation aimed at ensuring fair access, control, and use of data across businesses, consumers, and public institutions in the EU. It also seeks to balance fairness and legitimate data management with unlocking the economic potential of data. While it does not directly regulate profiling, it significantly impacts who can access and use data for profiling purposes by addressing data sharing and ownership. Alongside the DSM, the Data Act **prevents dominant players** (gatekeepers) **from monopolizing data access**.

At its core, the Data Act governs **machine-generated data**, particularly from **Internet-of-Things (IoT)** products and related services, establishing rules on who can collect, share, and utilize this data. Since profiling often relies on large-scale data processing, the Act influences profiling practices by clarifying data access rights and targeting fairness in data transactions. It also introduces safeguards to prevent stronger market players from imposing unfair data-sharing terms, ensuring that seeking for smaller entities to be able to compete in the data economy.

Additionally, the Data Act indirectly shapes profiling regulations by setting limits on **public-sector access to business-held data**. Additionally, it establishes protections against **unauthorized foreign access to EU non-personal data**, reinforcing EU data sovereignty and ensuring compliance with broader privacy and data governance frameworks.

By structuring data access and governance, the Data Act plays a crucial role in defining who controls the data that fuels profiling systems, ensuring that profiling is conducted within a transparent and competitive framework aligned with EU regulatory safeguards.

(1) Defining Features & Characteristics

i. Definition and Context

The **Data Act** is primarily concerned with **data access, sharing, and governance**, rather than profiling. However, it indirectly impacts profiling regulations by ensuring data minimization, restricting third-party use of data for profiling, and preventing manipulative practices.

The **Data Act refers to the GDPR's definition of profiling**,[132] reinforcing its alignment with EU data protection principles.

The Data Act **ensures that data made available under its provisions cannot be used for profiling**, except under strict conditions. It introduces safeguards against **excessive data retention, dark patterns, and foreign government access**. These key features are further explored in the sections following:

ii. User's Right to Share Data

The **Data Act** strengthens individuals' and businesses' **control over their data** by ensuring that users have the **right to share data with third parties**. If you use a smart device (IoT product)—like a connected car, smart home device, or industrial sensor—the Data Act ensures that data subjects control the data it generates. Data subjects have the right to share this data with a third party of your choice (e.g., a repair service or analytics provider) without the manufacturer interfering or restricting access.

- Right to Data Sharing:[133] Users, or authorized third parties acting on their behalf, can request that data holders provide **readily available data**, including metadata, in a structured, machine-readable format and, when feasible, in real-time. Data sharing must be free of charge to the user and meet the same quality standards as those available to the data holder.
- Restrictions on Gatekeepers:[134] Companies designated as **gatekeepers under the DMA cannot** act as third-party recipients under this provision, preventing dominant platforms from leveraging shared data to reinforce their market power.

iii. Restrictions on Profiling & Data Minimization

The **Data Act explicitly restricts profiling by third parties**, reinforcing the data minimization principle to prevent exploitative data use.

- Agreed Purpose & Deletion:[135] Third parties receiving data **must process it only for agreed-upon purposes** and erase it when no longer necessary.
- Ban on Profiling:[136] Third parties **cannot use received data for profiling**, except when it is **strictly necessary** to provide the service requested by the user.
- User Control & Consent:[137] Third parties can only share data with another entity **if the user explicitly agrees**. It must be **as easy to revoke access** as it was to authorize it.

---

[132] Regulation 2023/2854, of the European Parliament and of the Council, on Harmonised Rules on Fair Access to and Use of Data and Amending Regulation 2017/2394 and Directive 2020/1828 (Data Act), 2023 O.J. (L 2854) 1 ("Data Act") at Art 2.20.
[133] Data Act Art 5.1.
[134] Data Act Art 5.3.
[135] Data Act Art 6.1.
[136] Data Act Art 6.2(b).
[137] Data Act Recitals 37-39.

- No Profiling for Competitive Advantage:[138] Data received under the Data Act **cannot be used to develop a competing connected product**, ensuring fair innovation while preventing monopolistic data practices.

iv. Dark Patterns & Manipulative Design

The **Data Act** follows the **DSA's approach** by addressing **dark patterns**, noting its intention that users retain **genuine control** over their data-sharing choices. Third parties and data holders **cannot manipulate users into sharing data** through deceptive or coercive interface designs.

- Transparency in Digital Interfaces:[139] Users must be able to **exercise their rights freely**, without **non-neutral choices, coercion, or misleading nudges** influencing their decisions. By addressing deceptive data-sharing tactics, the Data Act pursues that **profiling and data-driven decision-making are based on freely given user consent**.

v. Gatekeepers & Data Sharing

The **Data Act** reinforces the **Digital Markets Act (DMA)** by **limiting the monopoly of gatekeepers' access to user-generated data**, ensuring that dominant digital platforms cannot use their market power to gain unfair competitive advantages.

Exclusion from Data Access Rights:[140]

The Data Act requires data holders to make readily available data when it is requested by a user, or third parties on behalf of users. However, gatekeepers are excluded from this data sharing mechanism.

- **Gatekeepers Cannot Request or Receive User Data**: Any company designated as a gatekeeper under the DMA cannot request, be granted, or commercially incentivize access to data generated by users.
- **No Circumvention via Third Parties**: If a third party gains access to data at the user's request, it cannot pass that data to a gatekeeper, nor can it subcontract services to a gatekeeper to indirectly facilitate access.

Impact on the Data Economy:[141] This provision is **rooted in competition policy**, acknowledging that gatekeepers **already control vast amounts of data** and **hold entrenched market power**. Allowing them to access additional user-generated data under the Data Act **would be disproportionate** and **counterproductive** to the regulation's goal of **balancing data value distribution**. **SMEs are exempt** from certain data-sharing obligations, preventing excessive regulatory burdens on smaller players.

Data acquisition through lawful means: At the same time, this restriction **does not prevent gatekeepers from acquiring data through lawful means**, such as voluntary agreements with

[138] Data Act Recital 39.
[139] Data Act Recital 38.
[140] Data Act Art 5; Recital 40.
[141] Id.

data holders, ensuring that they remain active market participants without unfairly benefiting from mandated data access rights.

vi. Safeguards Against Foreign Government Access

The Data Act introduces conditions on **international access to EU-held data**, protecting it from **third-country governmental interference**.[142]

- Blocking Unlawful Foreign Access: Data holders must **prevent international and third-country governmental access and transfer of non-personal data held in the Union**, if this would create conflict with EU or Member state law. This includes judgments by foreign courts and tribunals.
- Legal Review of Foreign Requests: If a **third-country court or authority** demands data, and there is no relevant treaty or international agreement, compliance is only permitted if:
    - The request is **proportional and specific**.
    - The data provider has **a right to challenge the request**.
    - The ruling **considers EU laws and protections**.
- EU Oversight & Advisory Role: The **European Data Innovation Board (EDIB)** and **national legal bodies** oversee compliance and can advise companies on whether a request violates EU law.

These safeguards ensure that non-personal data governed by the Act cannot be exploited by foreign governments, reinforcing EU sovereignty over its data economy and **preventing profiling by entities absent EU data processing standards**.

(2) Sectorial Classification

The **Data Act** does not directly regulate profiling but fundamentally shapes who can access and use data for profiling purposes**.** By structuring data access and its governance, it sets limits on how businesses, public institutions, and dominant digital players can leverage machine-generated data. These restrictions ensure that profiling remains constrained within transparent, fair, and competitive parameters—preventing data monopolization, manipulative data practices, and profiling-driven exploitation, inclusive of that from foreign entities.

i. Business

The Data Act regulates profiling in business contexts through its data governance ramifications.

- **User-Owned Data & Profiling Restrictions**: Users retain legal rights of control over data generated by their connected products (IoT devices, industrial sensors, smart home systems). While users can share this data with third parties, businesses receiving it cannot use it for profiling unless strictly necessary to provide the requested service.[143] This prevents third-party profiling beyond the original purpose of data collection**.**
- **Prevention of Gatekeeper-Controlled Profiling & Fair Competition**: The Act bars gatekeepers from requesting, receiving, or indirectly acquiring user-generated data

[142] Data Act Art 32; Recitals 102-103.
[143] Data Act Art 6.2(b)

through third parties.[144] Since gatekeepers already process vast amounts of personal and behavioral data, restricting their ability to collect additional profiling-relevant data limits their ability to reinforce their dominance through data-driven user targeting. Profiling relies on data scale, meaning that businesses with exclusive or unequal access to key data sources gain a significant market advantage.

ii. Social

The Data Act introduces protections to ensure that profiling does not exploit individuals, particularly in data-driven decision-making, manipulative digital design, and government data access**.**

- **User Consent & Data Minimization in Profiling**:[145] Users must explicitly agree before third parties can access their data, and they can just as easily revoke access. Profiling based on machine-generated data cannot be conducted without informed, revocable user consent**.** The Data Act addresses automated decision-making based on user-generated data, which cannot be deployed for profiling unless it is strictly necessary to fulfill a user-requested service
- **Dark Patterns & Manipulative Interfaces**: [146] Deceptive digital design, such as nudging users into sharing data for profiling or making refusal options harder to find, is addressed. This aligns with DSA regulations on manipulative platform design, intending that profiling and behavioral tracking remain based on genuine user choices rather than coercion or misleading interfaces**.**
- **Public-Sector Data Access**:[147] The Data Act limits how government institutions can access business-held data–intending that such access cannot be exploited for mass profiling or surveillance beyond its intended purpose, but also allowing emergency or public interest data access.

iii. Political

The Data Act safeguards profiling in political and governmental contexts by preventing mass-scale profiling via unauthorized data access both from internal governmental action as well as from foreign entities, ensuring that profiling-based decision-making remains subject to EU legal protections**.**

- **Foreign Government Access to Data for Profiling**:[148] The Data Act prevents third-country governments from accessing EU non-personal data without going through proper legal channels. This can protect against foreign intelligence operations, politically motivated profiling, election interference via data-driven voter targeting, but in essence, it intends to ensure that sharing, gathering, and processing of data is (i) lawful in its acquisitions, and (ii) subject to EU standards and.

[144] Data Act Art 4.3, Recital 39.
[145] Data Act Art 6.2, Recital 39.
[146] Data Act Recital 38.
[147] Data Act Chapter V.
[148] Data Act Art 32.

- **Public Data Use Must Comply with Profiling Restrictions**: [149] Public-sector institutions cannot access privately held data for profiling-based decision-making, except in legally justified, strictly necessary cases such as public emergencies. This aligns with GDPR safeguards against excessive government profiling while still allowing public interest data use within legal constraints.

3.7 Commission Staff Working Document: Fitness Check of EU Consumer Law on Digital Fairness

The Commission Staff Working Document: Fitness Check of EU Consumer Law on Digital Fairness (Fitness Check) is not a legal prescriptive document, but a comprehensive assessment of the EU's core consumer protection laws functionality and gaps in the evolving digital landscape. While the EU legal framework has long aimed to ensure fairness and empower consumers, the rapid growth of AI, big data, and digital business models has introduced new risks. These developments have raised concerns that technological advancements are being used to distort consumer decision-making, manipulate behavior, and undermine trust in digital markets.

This Fitness Check evaluates three key Directives that serve as the foundation of EU consumer protection law:

- **Unfair Commercial Practices Directive (UCPD) (2005/29/EC):** Regulates misleading and aggressive marketing practices.
- **Consumer Rights Directive (CRD) (2011/83/EU):** Defines consumer rights in contracts and digital transactions.
- **Unfair Contract Terms Directive (UCTD) (93/13/EEC):** Prevents businesses from imposing unfair terms in consumer agreements.

The evaluation is largely **retrospective**, assessing whether these laws remain effective in digital markets and whether they provide sufficient safeguards against exploitative digital practices. However, the assessment also includes a **forward-looking** element, identifying regulatory gaps, inconsistencies, public perception, and areas where the rules may need adaptation to emerging risks—such as **dark patterns, algorithmic decision-making, and behavioral profiling**.

As digital markets evolve, so do the methods businesses use to engage with consumers. The Fitness Check examines whether current consumer protection laws are fit for purpose in an era of personalized advertising, predictive analytics, and AI-driven persuasion techniques. It also explores whether additional measures are needed to **strengthen consumer autonomy, prevent digital manipulation, and ensure fairness in online transactions**.

Below is an analysis of the key aspects of the Fitness Check, its findings, and its implications for profiling, consumer choice, and digital fairness.

[149] Data Act Chapter V.

(1) Key Aspects

The Fitness Check evaluates the adequacy of EU consumer protection laws in an era of AI-driven personalization where behavioral targeting and manipulative commercial practices are an increasingly precise risk. It assesses whether current frameworks effectively safeguard consumers from **dark patterns, addictive design, and asymmetric market power**, particularly as businesses gain increased influence over consumer decision-making through algorithmic profiling.

The report raises a fundamental question: **Are existing consumer laws sufficient to address AI-driven persuasion and profiling, or do they need stronger prohibitions on manipulative and exploitative practices?**

i. Personalization & Consumer Autonomy

Personalized recommendations, pricing, and advertising are (i) increasingly shaping consumer experiences in the digital marketplace and (ii) shift control toward businesses, potentially reinforcing market imbalances.[150] While personalization can offer benefits, it also raises serious concerns about consumer control, fairness, and trust.

- **Power concentration among data-dominant firms**: Businesses with advanced profiling capabilities can shape consumer behavior in ways consumers cannot easily counteract.
- **Consumers lack insight into algorithmic personalization**: Many feel that AI systems, not personal choice, dictate their digital experiences. 74% of consumers believe their personal data has been misused to personalize commercial offers,[151] and 66% are concerned about data collection and profiling practices.[152] With regards to data-to-profiling conversion specifically, 38% of consumers reported difficulty understanding the type of profile platforms generated about them based on their personal data and how it influenced the content they were shown. [153]
- **Blurred boundaries between information & advertising**: There is an increasing difficulty distinguishing between genuine content and targeted marketing, raising risks of covert manipulation.

ii. Dark Patterns & Algorithmic Persuasion

Dark patterns and manipulative personalization strategies can distort consumer decision-making, resulting in financial harm, diminished autonomy, and privacy concerns. These practices also contribute to cognitive burdens and potential mental distress while raising broader concerns about market fairness, price transparency, and consumer trust in digital commerce.[154] Some specific features include:

---

[150] Fitness check at 21 et seq.
[151] Fitness Check at 21.
[152] Id.
[153] Fitness Check at 142.
[154] Fitness Check at 30 et seq.

- **Psychological pressure & targeting through UI/UX and information presented**: Many digital interfaces nudge users into purchases they would not have otherwise made, often through forced actions, false urgency, or misleading scarcity cues. Consumers report feeling confused (40%) and pressured (35%) by exposure to dark patterns.[155]
- **Physiological responses**: Experimental studies show that dark patterns can trigger anxiety, reduce cognitive control, increase susceptibility to manipulation, increase heart rates, and impair decision-making, particularly when paired with personalized targeting.[156]
- **Normalization of deceptive practices**: Frequent exposure makes manipulative design seem like an unavoidable part of digital life. A key concern is that consumers have begun to accept manipulative interfaces as normal, making them less likely to detect or challenge unfair digital practices.[157]

iii. Addictive Design & Consumer Dependency

Commercial strategies that maximize engagement—such as infinite scroll, autoplay, loot boxes, and algorithmic recommendation loops—are increasingly linked to mental health concerns, compulsive behaviors, and digital dependency.[158]

- **Attention as a business model**: Platforms monetize consumer engagement, encouraging longer usage for monetization or increased data collection.
- **Potential health impacts**: Research links compulsive digital engagement to anxiety, cognitive fatigue, and disrupted sleep patterns.
- **Regulatory gap**: While laws protect against misleading practices, they do not address commercial exploitation of compulsive behaviors.

iv. Asymmetric Positioning & Market Power

Advances in technology enable businesses to consolidate their market power, often at the expense of consumer autonomy. AI-driven personalization further skews market dynamics, reinforcing structural imbalances between traders and consumers by subtly shaping decision-making in ways that consumers may neither fully perceive nor control.[159]

- **Businesses can predict and influence consumer behavior**: Advanced algorithmic profiling allows traders to shape decision-making in ways consumers may not fully perceive.
- **Reduced consumer agency**: Many feel they do not control their digital choices, as AI-driven systems determine what they see, buy, and engage with.

v. Vulnerable Consumers in the Digital Age

Vulnerable consumers—such as those with limited digital literacy, minors, or individuals experiencing emotional distress—face heightened risks in the digital marketplace.

---

[155] Id.
[156] Id.
[157] Id.
[158] Fitness Check at 30 et seq.
[159] Fitness Check at 129.

Characteristics like credulity, mental or physical infirmity, or age make them particularly susceptible to manipulative design strategies. Addictive design, algorithmic personalization, and engagement-maximizing techniques increase the likelihood of compulsive behavior and data exploitation. Many of these consumers may struggle to recognize or resist digital tactics engineered to capture attention, making them more vulnerable to both psychological and financial harms.

Additionally, digital markets exacerbate consumer vulnerabilities, particularly for individuals experiencing financial insecurity, emotional distress, or limited technological awareness. The evolving digital landscape allows businesses to assess consumer behaviors in real time, reinforcing existing disparities through targeted strategies that influence decision-making. Some key characteristics of these interactions are:

- **Dynamic nature of vulnerability:** Vulnerability is not only demographic but also situational, shaped by real-time consumer behavior and algorithmic profiling.
- **Profiling-based exploitation:** Businesses can detect when consumers are in distress or financially insecure, leveraging this information to push high-pressure sales tactics.
- **Need for explicit protections:** Some national authorities advocate for direct prohibitions on commercial practices that exploit consumer distress, cognitive biases, or temporary emotional states.

vi. Technological Developments & Future Risks

The rapid evolution of AI and digital technologies is reshaping consumer markets, introducing new complexities and vulnerabilities. While AI-driven personalization and automation offer efficiencies, they also create asymmetries in decision-making power between businesses and consumers. The Fitness Check highlights several key technological developments that challenge the current consumer protection framework:[160]

- **Generative AI & misleading content**: AI-generated materials blur the distinction between factual information, marketing, and manipulation. Consumers may struggle to discern whether they are engaging with genuine content or algorithmically generated outputs designed to influence their decisions.
- **Emotion-Recognition AI & Persuasive Interfaces**: AI systems that analyze emotions and simulate human interaction could increase psychological influence over consumers, creating a new layer of behavioral manipulation. Even when consumers are aware they are interacting with AI, these systems may distort decision-making by fostering trust or urgency artificially.
- **Automated Contracting & Smart Contracts**: AI-powered contracts and automated decision-making in transactions raise concerns about consumer over-reliance on systems they may not fully understand. If consumers lack the ability to challenge unfair terms or errors, their agency in contractual relationships diminishes.
- **Digital infrastructure shifts**: The proliferation of connected devices, edge computing, and virtual reality environments, alter the consumer-trader dynamic. These changes raise

[160] Fitness Check at 82 et seq.

questions about how fundamental consumer protections—such as transparency, informed consent, and contractual fairness—should be applied in evolving digital contexts.

(2) Gaps & Next Steps

The Fitness Check highlights several areas where existing consumer protection frameworks may be insufficiently prepared for new technological and market challenges. While current regulations provide a foundation for fairness and transparency, gaps remain in their ability to tackle evolving risks posed by AI-driven personalization, data-driven manipulation, and asymmetric market power. The following section outlines key regulatory shortcomings and potential avenues for future policy development.

i. Regulatory Gaps & the Limits of Transparency

A key finding of the Fitness Check is that many AI-driven personalization strategies, even when manipulative, are not explicitly illegal.[161] This can have complex commercial and regulatory implications. Additionally, the burden of proof to show harm from these patterns may be anchored in prior technological dynamics:

- **Transparency ≠ fairness**: Businesses can comply with disclosure rules while still using aggressive profiling techniques.
- **Challenges in proving harm**: Consumers struggle to demonstrate when AI-driven marketing crosses ethical or legal boundaries.

This raises the question: **Should AI-driven personalization be presumed unfair when it distorts consumer decision-making, even if transparency requirements are met?**

ii. Next Steps & Policy Considerations

The Fitness Check questions whether consumer protection laws are adequate in addressing AI-driven asymmetries in decision-making, persuasion, and market power, or if an evolution is necessary. Some data and profiling-related conclusions include:

- **Strengthening consumer protections, expanding blacklisted practices**: Proposals include banning specific profiling techniques that create psychological pressure or exploit vulnerabilities. This call includes explicit prohibitions on manipulative AI-driven marketing and psychographic profiling, with key efforts dedicated to expanding the UCPD blacklist to ban psychographic profiling, behavioral manipulation, and exploitation of vulnerabilities.
- **Rebalancing the burden of proof**: Businesses may be required to demonstrate that their AI-driven personalization strategies are fair, rather than placing the burden on consumers.

The Fitness Check identifies several core challenges in ensuring consumer protection in the digital environment. While existing directives remain relevant, their effectiveness is increasingly tested by **AI-driven personalization, manipulative design, and profiling-based commercial**

[161] Fitness Check at 164.

practices. The document assesses how these practices impact consumer autonomy, trust, and decision-making, with particular attention to vulnerable consumers.

4. Recommendations for Japan

As AI-driven profiling becomes increasingly embedded in economic, social, and political spheres, nations are seeking to provide effective responses to the interactions of these novel technologies with markets, elections, and fundamental rights. Japan plays a central role in global AI governance, having led and contributed to key initiatives such as the G7 Hiroshima AI Process or the Bletchley Declaration. Domestically, Japan aims to regulate AI in a way that safeguards human rights and democratic principles while fostering economic growth.

To be effective, regulatory frameworks addressing AI profiling should develop a structured, adaptive, and principle-driven regulatory framework that balances technological innovation, consumer protection, and market competitiveness. Regulation should neither stifle AI's potential for economic growth nor allow unchecked profiling practices that undermine individual autonomy, social equity, or market fairness.

Japan's regulatory approach should establish clear legal obligations, enforceable accountability mechanisms for businesses, and strong protections for individual rights. This will ensure that AI-powered personalization and decision-making remain transparent, fair, and aligned with democratic and economic priorities. This section outlines core principles—drawing on the EU's AI-profiling regulatory architecture—that could provide insights for Japan's policy development, ensuring that any future approaches are not only reactive but also forward-looking and capable of evolving alongside technological and geopolitical shifts.

This section will provide (1) foundational considerations for the integration of AI-profiling technologies into the regulatory system, as well as (2) specific actionable recommendations for the development of regulatory mechanisms, to ensure AI-profiling that serves society economically, socially, and politically.

1. Foundational Considerations for Japan's AI Profiling Regulation

As Japan refines its regulatory approach to AI-driven profiling, several foundational considerations should shape its framework. These principles ensure that regulation is both effective and adaptable, balancing economic growth, technological advancement, and fundamental rights. Key considerations include:

- **Balancing Innovation, Economic Growth, and Fundamental Rights** – Ensuring AI profiling fosters technological and economic development while safeguarding individual rights and consumer protections.
- **Building Trust Across Stakeholders** – Establishing legal certainty for businesses, strong consumer protections, and effective institutional oversight to maintain public confidence.
- **Regulating Both Private and Public Sector Profiling** – Applying consistent standards to prevent unchecked power in commercial and governmental AI applications.

- **Ensuring Market Growth, Social Equity, and Political Integrity** – Addressing data processing and utilization governance in order to ensure AI-driven profiling is an economic asset, does not reinforce inequalities, and safeguards democratic reliability.
- **Corporate Accountability and Individual Rights** – Establishing both enforceable obligations for businesses and actionable rights for individuals affected by AI decisions.
- **Moving Beyond Principles to Concrete Action** – Translating ethical AI frameworks into pathways with effective enforcement mechanisms.
- **Capitalizing on the Data-Sharing Economy While Protecting User Autonomy** – Encouraging responsible data sharing while ensuring individuals retain meaningful control over their data.
- **International Coordination in Data Governance** – Aligning Japan's approach with global AI regulations to ensure interoperability and cooperation.
- **Addressing Data Asymmetries** – Preventing excessive power imbalances between corporations and individuals, as well as between dominant firms and smaller businesses.
- **Ensuring Agile and Adaptive Governance** – Creating a regulatory framework that evolves alongside technological advancements and geopolitical shifts.

These foundational elements provide the basis for a regulatory strategy that is forward-looking, responsive, and capable of mitigating the risks of AI-driven profiling while maximizing its benefits.

i. Balancing Competing Priorities: Innovation, Economy, and Fundamental Rights

The AI policy debate generally, and AI-driven profiling in particular, operate at the crossroads of technological progress, economic opportunity, and societal impact. Regulation must recognize and balance these dimensions, ensuring that AI-driven personalization strengthens market efficiency while safeguarding individual rights and social equity. Japan should establish rules that:

- Encourage Innovation: Encourage AI innovation and global competitiveness by setting clear yet adaptable guidelines that allow businesses to develop AI-driven profiling tools responsibly, ensuring transparency, accountability, and ethical deployment while preventing regulatory overreach that could stifle business agility.
- Foster the Economic Potential of AI: AI-driven profiling can enhance productivity, optimize market efficiencies, and drive economic growth by improving consumer engagement, streamlining decision-making processes, and enabling businesses to offer more precise and adaptive services. Regulatory frameworks should support AI's role in economic expansion by fostering an environment where businesses can leverage data-driven personalization without excessive regulatory friction, ensuring that innovation translates into tangible economic benefits.
- Guarantee Fundamental Rights: Ensure AI-driven personalization aligns with human agency and fundamental rights by establishing protections against manipulative or opaque decision-making processes that undermine consumer autonomy, data-subject rights, or create asymmetrical power dynamics between businesses and individuals. AI

systems should enhance user control rather than shape consumer behavior in ways that diminish informed decision-making.

ii. Building Trust Across Stakeholders: Industry, Individuals, and Public Institutions

For AI regulation to be effective, it must **build trust and address the intent from all key stakeholders**—industry, individuals, and regulatory and enforcement institutions. AI-driven profiling presents challenges in **legal certainty, enforcement, and public confidence**, requiring a governance model that provides:

- Legal Certainty: Provides clear, enforceable guidelines to enable business compliance without paralyzing regulatory burdens.
- User-Centric Data Control: Strengthens consumer rights protections, giving individuals meaningful consensual control over their data and AI interactions.
- Institutional Development & Involvement: Enhances **institutional oversight capacity**, ensuring that **both corporate and governmental profiling practices** are transparent, accountable, and compliant with regulatory safeguards.

iii. Regulating Profiling Across Private and Public Sectors

Comprehensive and encompassing AI profiling regulation must include provisions for (i) **private-sector applications**, and (ii) **government use of profiling technologies**. Corporate activity and governmental action raises risks concerning market performances, as well as surveillance, discrimination, and unchecked decision-making. Accordingly, regulatory frameworks should:

- **Apply consistent standards** to both corporate and government profiling, ensuring transparency, fairness, and **safeguards against exploitative or discriminatory AI-driven personalization**.
- **Address private-sector AI profiling** with clear obligations on data use, transparency, and limits on excessive or manipulative personalization techniques.
- **Regulate public-sector AI profiling**, ensuring government use of AI-driven decision-making does not lead to excessive surveillance or discriminatory outcomes.

iv. Economic Growth, Social Equity, and Political Integrity

Regulation must differentiate between **economic, social, and political implications** of profiling to ensure balanced governance:

- Economic: Profiling and AI-driven personalization create market efficiencies but must be regulated to prevent monopolistic data control and unfair market concentration.
- Social: AI profiling should not reinforce **i**nequality, discrimination, or consumer vulnerabilities—systems must be evaluated for bias, and protections should extend to marginalized groups and sensitive data categories.
- Political: Algorithmic content curation and political micro-targeting must be monitored to ensure they do not distort democratic processes, spread misinformation, or erode civic engagement.

v. Corporate Accountability and Individual Rights

AI-profiling frameworks must establish **a dual structure of AI governance**, one that (i) establishes corporate accountability and (ii) ensures individuals have AI-specific rights. Regulation should:

- Require **businesses to implement responsible AI risk management, transparency, and audit mechanisms** to prevent exploitative profiling.
- Grant **individuals AI rights**, for data-subject to be able to present actionable causes when confronted with non-compliant AI-profiling overreach or harm.

vi. Moving Beyond Principles: Ensuring Regulatory Implementation

While **ethical AI principles** have laid the groundwork for responsible AI governance, regulatory frameworks must now translate them into **enforceable obligations**. Regulators should:

- Establish **binding compliance requirements** for businesses using AI-driven personalization.
- Clear Define **clear legal criteria for manipulative, damaging, or unfair profiling practices**.
- Introduce **agile regulatory mechanisms** that allow for periodic review and adaptation as AI technologies evolve.

vii. The Data Economy: Risks and Opportunities

The data-sharing economy presents a complex balance of economic potential, consumer rights, and regulatory challenges. It offers opportunities for innovation, competition, and public sector advancements but also raises concerns over privacy, market concentration, and ethical governance. Striking the right balance requires fostering data-driven growth while ensuring individuals and businesses retain control over how data is used.

- **Opportunities**: Some of the opportunities associated with the data economy are the following:
    - Economic Growth & Innovation: AI-driven personalization and data analytics can improve business efficiency, enable new market entrants, and enhance product and service offerings, driving economic expansion.
    - Enhanced Consumer Experiences: Personalization can improve user satisfaction by tailoring content, recommendations, and services to individual preferences.
    - Data-Driven Competition: If managed correctly, data-sharing frameworks can create a more level playing field, allowing small and mid-sized businesses to compete with data-dominant firms, fostering innovation and preventing monopolistic control.
    - Smarter Public Policy & Infrastructure Planning: Governments can leverage aggregated, non-personal data to improve urban planning, public health responses, and transportation efficiency, leading to better resource allocation and more effective public services.
- **Risks**: Alongside the opportunities, risks include:

- Data Monopolization & Market Asymmetry: Large firms with extensive data access can entrench their dominance, limiting competition and restricting market entry for smaller businesses.
- Loss of Consumer Control & Privacy Risks: Without clear protections, individuals may lose control over how their data is used, facing invasive profiling and exploitation of personal vulnerabilities.
- Regulatory & Ethical Challenges: Balancing the economic benefits of data-sharing with fundamental rights requires careful governance to prevent excessive data extraction, ensure transparency, and mitigate potential harms, such as unfair discrimination and algorithmic biases.
- Government Overreach & Surveillance Risks: Public sector access to vast data pools could lead to excessive monitoring, mass surveillance, or misuse of AI-driven profiling in ways that undermine civil liberties and democratic freedoms.

viii. Global AI and Data Governance Cooperation

AI-driven profiling is not a national issue—it requires **global regulatory coordination**. Japan should align its approach with **international best practices** to ensure:

- **Interoperability with global AI governance efforts** (e.g., EU AI Act, OECD AI principles, G7 AI guidelines).
- **Cross-border data governance mechanisms**, preventing fragmented and conflicting regulatory approaches.
- **Strategic engagement with international partners**, ensuring **Japan's regulatory approach remains competitive and informed by emerging global AI risks**.

ix. Addressing Data Asymmetries: Corporate Power & Individual Rights

There are two major power asymmetries in AI-driven profiling that must be addressed:

1. The imbalance between corporations and individuals: Large platforms collect vast amounts of personal data, making it difficult for individuals to understand, contest, or avoid profiling practices.
2. The dominance of data-rich firms over smaller businesses: Data-driven personalization is a **powerful economic asset**, which can present competition and barriers-of-entry issues to certain industry if infrastructure and data gathering and processing is centralized. To this effect, regulation should:
    - Ensure **users have meaningful choices** regarding how their data is used.
    - Prevent **dominant firms from leveraging cross-service data unfairly**.
    - Introduce **fair access provisions** for smaller businesses to participate in AI-driven personalization markets.

x. Sector-Specific Protections & Differentiated Compliance

AI-driven profiling does not operate uniformly across industries. **Different sectors present distinct risks**, ethical considerations, and regulatory needs. While profiling in healthcare may pose risks of discrimination in medical treatment, profiling in finance may lead to unfair credit

access, and in employment, it may reinforce bias in hiring processes. Similarly, law enforcement and biometric surveillance present significant civil rights concerns.

To develop effective, risk-calibrated governance, regulatory frameworks should recognize these differences and consider sectorial flexibility rather a one-size-fits-all approach. Policymaking could consider:

- Sector-Specific Risk Exposure: High-risk sectors (e.g., criminal justice, healthcare, and elections) require stricter compliance obligations, while lower-risk applications (e.g., content recommendations, personalized retail experiences) can operate under more flexible frameworks.
- Tailored Transparency & Accountability Mechanisms: What constitutes meaningful explainability in AI profiling varies by sector—healthcare decisions may require medical-grade justifications, while financial profiling may require clear consumer opt-out rights.
- Proportional Enforcement & Oversight: Sectorial regulators should play a key role in monitoring AI profiling within their domain, ensuring that compliance measures are adapted to each field's specific risks and challenges.
- Public-Private Collaboration & Industry Self-Regulation: Collaboration between regulatory bodies and industry stakeholders could play a role in shaping effective AI governance. Industry-driven standards, voluntary guidelines, and self-regulatory frameworks have the potential to complement formal regulation, particularly in rapidly evolving sectors where rigid legal requirements may struggle to keep pace with technological advancements. Encouraging cooperation between public and private actors may help balance innovation with accountability while fostering responsible AI development.

xi. Regulatory Agility and Adaptability

Regulating AI-driven profiling requires a governance framework that is dynamic, responsive, and capable of evolving alongside technological, economic, and geopolitical shifts. AI systems develop rapidly, often outpacing existing legal structures, while market forces and global regulatory landscapes continue to change. A rigid, one-size-fits-all approach risks becoming obsolete or stifling innovation, whereas an overly permissive system may fail to protect fundamental rights and market fairness. Effective regulation must strike a balance—providing legal certainty while allowing for ongoing adaptation to new risks and opportunities.

AI-driven profiling is constantly evolving, requiring regulatory flexibility to address:

- **Technological advancements**, as AI models become more sophisticated, capable of deeper behavioral analysis, and increasingly embedded in everyday decision-making.
- **Economic shifts**, as data-driven markets grow and data becomes an increasingly valuable economic asset, influencing competition, consumer behavior, and the role of AI in shaping digital economies.

- **Geopolitical developments**, as nations establish divergent approaches to AI governance, affecting cross-border data flows, regulatory harmonization, and global market dynamics.

Governance structures should be **designed to evolve**, incorporating:

- **Periodic regulatory reviews**, ensuring that legal frameworks remain relevant to emerging AI capabilities and uses, and market realities.
- **Regulatory sandboxes**, enabling controlled testing environments for AI-driven personalization, allowing policymakers to assess risks and benefits before imposing strict rules.
- **Adaptive and iterative compliance frameworks**, fostering dialogue between regulators, businesses, and civil society to ensure enforcement mechanisms remain effective without impeding responsible AI innovation.

2. Recommendations for AI-Profiling Regulation in Japan

Japan has a critical opportunity to shape the future of AI-driven profiling by establishing a regulatory framework that is both pragmatic and future-ready. As AI becomes more deeply embedded in commercial, social, and political systems, regulation must ensure that technological advancement is economically dynamic, as well as serves human needs rather than dictating them. This means safeguarding individual rights; ensuring market, social, and political fairness; and maintaining public trust, all while fostering AI-driven economic growth and innovation.

The following recommendations provide a structured approach to AI profiling regulation, addressing both immediate risks and long-term governance challenges. These measures focus on:

- **Building AI-Specific Rights** – Establishing actionable and enforceable rights for individuals to manage, challenge, and opt out of AI-driven profiling.
- **Safeguarding Sensitive Data and Protecting Vulnerable Populations** – Establishing robust protections to prevent the misuse of sensitive data and ensure that profiling does not exploit, discriminate against, or unduly influence vulnerable individuals.
- **Risk-Based Compliance and Proportional Regulation** – Applying tiered regulatory obligations, with stricter oversight for high-risk applications and data-dominant firms while maintaining flexibility for startups and low-risk AI uses.
- **Ensuring Data Control: Strengthening Corporate and Public-Sector Accountability** – Establishing clear obligations for both private and public sector entities in their data gathering, processing, and management structures, to uphold transparency, fairness, and responsible AI profiling practices, ensuring individuals retain meaningful control over their data.
- **Promoting a Fair and Competitive Data-Sharing Economy** – Encouraging responsible data use while preventing monopolistic control over AI-driven personalization markets.
- **Preventing Manipulative AI Practices and Dark Patterns** – Prohibiting deceptive, coercive, or exploitative AI-driven personalization techniques that manipulate consumer behavior.

- **Embedding Compliance Throughout the AI Lifecycle** – Implementing pre-market certification, continuous auditing, and adaptive regulatory tools to ensure ongoing accountability.
- **Enhancing Japan's Role in International AI Governance** – Aligning with global regulatory frameworks while maintaining sovereignty over AI and data governance policies.
- **Robust Enforcement and Regulatory Agility** – Ensuring compliance mechanisms are effective, proportionate, and capable of adapting to emerging risks and technological developments.

By selectively and contextually integrating these targeted recommendations, Japan can build a regulatory system that protects individual rights, promotes market fairness, and positions itself as a global leader in AI governance.

i. A Rights-Based Approach to AI Profiling

AI-driven profiling must be **rooted in individual rights**, ensuring that people maintain meaningful control over how their data is used. Regulations should establish **actionable and enforceable protections** that allow individuals to challenge, modify, or opt out of AI-based decisions.

- **Data Ownership & Control:** Users should have the legal right to own and manage their personal data, making it actionable against both corporations and government entities.
- **Transparency & Explainability as a Right:** In addition to transparency being a compliance requirement for corporate governance, individuals must be able to demand clear explanations of how AI-driven profiling affects them, ensuring they are not subject to opaque or unaccountable decision-making.
- **AI & Profiling Rights:** AI-specific rights should be developed, so that data subjects can have effective redress mechanisms to counter profiling and algorithmic decision-making. Rights could include:
    - The **right to contest AI-driven decisions** that impact their economic, social, or political rights.
    - The **right to correct or modify profiling outcomes** that are inaccurate or unfair.
    - The **right to opt out** of AI-driven profiling, either entirely or for specific applications.
    - The **right to be free from profiling-based discrimination**, ensuring fairness in employment, finance, and essential services.

ii. Special Protections for Sensitive Data & Vulnerable Populations

AI-driven profiling can pose heightened risks when applied to sensitive personal data or vulnerable populations. Stronger safeguards should be implemented in cases where profiling could lead to **discrimination, exploitation, or undue influence** based on sensitive data categories or exercised upon vulnerable populations.

- Prohibited or Restricted Profiling**:** Certain types of profiling should be outright prohibited or subject to heightened restrictions, particularly where it targets or exploits vulnerabilities.
    - *Sensitive Data Protections*: Profiling based on race, ethnicity, political opinions, religion, health data, biometric data, or sexual orientation should be strictly regulated, with explicit legal bases and additional safeguards.
    - *Safeguards for Vulnerable Populations*: AI-driven profiling must not exploit vulnerabilities or reinforce systemic disadvantages. Protections should apply dynamically, recognizing that vulnerability is situational and evolving. Some target groups could include:
        - Children & Elderly: Protect those with limited digital literacy or decision-making capacity.
        - Individuals Lacking Capacity to Consent: Ensure AI does not override autonomy where informed consent is not possible.
        - People Experiencing Hardship: Prevent profiling that exploits financial distress, emotional vulnerability, or social disadvantage.

iii. Tiered Compliance for Agility & Risk Management

AI profiling regulation should be structured around proportionality. This means, that higher-risk applications and larger-impact players face higher compliance requirements, while lower-risk innovations and enterprises without large-scale or gatekeeping influence remain flexible and competitive. This approach targets regulation where it is most needed, ensuring stronger protections for high-impact uses of AI profiling while aiming to maintain economic dynamism and fairness. A tiered compliance model balances innovation with accountability by:

- Impact-and-Scale-Based Compliance: Regulations should be calibrated to reflect both the size of the entity and the scope of its AI profiling activities.
    - *Stronger Oversight for Dominant Players*: Major platforms and data-dominant firms with extensive profiling capabilities should meet stricter transparency, accountability, and fairness standards to prevent monopolistic data practices and consumer exploitation.
    - *Agility for Startups & SMEs*: Smaller businesses should have streamlined compliance requirements, ensuring regulatory burdens do not stifle innovation or competition.
- Graduated Safeguards Based on Profiling Risk: Compliance obligations should scale with the potential impact of profiling.
    - *Higher-Risk Profiling Requires Stricter Controls*: Profiling systems with significant consequences—such as employment decisions, creditworthiness assessments, biometric surveillance, criminal profiling, and political or ideological targeting—should be subject to fairness audits, heightened consent requirements, and, where necessary, outright prohibitions.

- *Lower-Risk Applications Should Have More Flexibility*: AI-driven personalization in areas with minimal societal impact (e.g., content recommendations, retail personalization) should remain lightly regulated, provided transparency requirements are met, and fairness in economic, social, and political interactions are respected.

iv. Strengthening Individual Control Over Data for AI Profiling

AI profiling regulation should ensure that individuals have material agency over how their data is used. This data-subject control should be based on (i) consent and (ii) data minimization. Both corporate and public-sector profiling must be subject to clear, enforceable safeguards that protect autonomy, privacy, and fairness in decision-making accordingly.

A. Corporate AI Profiling & Consumer Data Rights

- **Ensuring Meaningful User Autonomy**: Individuals should have practical, accessible mechanisms to manage how their data is collected and used in profiling, with clear choices rather than buried opt-outs or complex settings (dark patterns).
- **Accountability for AI-Driven Decision-Making**: Businesses must be responsible for ensuring AI profiling outcomes are explainable, contestable, and fair, with clear redress mechanisms for individuals affected by automated decisions.
- **Preventing Predatory Data Practices**: Regulations should prohibit coercive or deceptive data collection, ensuring that companies do not manipulate users into consenting to invasive profiling through dark patterns or misleading consent frameworks.

B. Public-Sector AI Profiling & Accountability

- **Strict Boundaries on Government Use of Profiling**: Public institutions must be held to data management standards, ensuring AI-driven profiling is not used for broad surveillance or discriminatory decision-making.
- **Transparency & Public Oversight**: Government profiling practices should be subject to independent oversight, public reporting requirements, and clear legal frameworks to prevent abuse and ensure due process.
- **Data Sharing Must Be Justified & Proportional**: Transfers of private-sector data to government agencies should be limited to well-defined public interest purposes, with strict safeguards on use, retention, and anonymization.

v. Enhancing & Protecting the Data Sharing Economy

The data-sharing economy presents both significant economic potential and regulatory challenges. Regulation should **enable innovation and fair competition** while ensuring individuals retain **meaningful control over their data** and are protected from exploitative practices.

This dynamic requires approaches including:

- **Unlocking the Potential of a Data-Driven Economy**: AI-driven personalization, fueled by data sharing, can enhance economic efficiency, innovation, and consumer experiences. Regulations should support responsible data use while safeguarding privacy and security.
- **Ensuring User Autonomy**: Users should have clear, enforceable rights over how their data is shared, ensuring that data transfers are voluntary and free from coercion.
- **Preventing Data Monopolization & Market Concentration**: Dominant platforms should not be able to hoard data access, restricting smaller businesses and startups. AI-driven personalization should benefit all market players, fostering competition and sustainable growth.
- **Interoperability & Fair Competition**: Regulations should prevent closed ecosystems, ensuring that smaller businesses can compete without being locked out of essential data markets.
- **Public Interest Data Use & Safeguards**: Certain non-personal data—such as aggregated data for public health, crisis response, or infrastructure planning—should be made accessible to governmental entities under strict safeguards to prevent misuse.

vi. Preventing Manipulative AI-Driven Personalization & Dark Patterns

AI-driven personalization must not be used to manipulate, deceive, or pressure consumers into making decisions against their best interests.

- **Protecting against AI-driven manipulation:** Hyper-personalized urgency tactics, deceptive framing, and AI-generated emotional pressure should be explicitly covered under consumer protection laws.
- **Regulating Dark Patterns in AI-Recommender Systems:** AI-driven platforms should not exploit behavioral biases to nudge users into unintended decisions.
- **Ensuring AI personalization enhances user control:** Profiling-based recommender systems should be transparent and designed to empower consumer choice, rather than limit it.

vii. Compliance Throughout the AI Lifecycle

AI profiling systems must be subject to continuous oversight and risk management, ensuring accountability **before, during, and after deployment.**

- **Pre-market certification:** High-risk AI profiling systems should undergo regulatory approval before deployment.
- **Regular auditing & monitoring:** AI systems must be evaluated for fairness, accuracy, and potential harms on an ongoing basis.
- **Adaptive regulatory tools:** AI oversight should incorporate automated enforcement mechanisms to detect violations in real time.

viii. Robust Enforcement & Accountability

Regulations are only effective if they are **properly enforced and adaptable** to the evolving nature of AI-driven profiling.

- **Proportionate enforcement**: Penalties should scale based on the severity of the violation to ensure meaningful deterrence.

- **AI-driven monitoring & audits**: Regulators should deploy automated compliance tools to track profiling practices and detect violations.
- **Stronger whistleblower protections**: Employees who report unethical AI-profiling practices should be legally safeguarded.

ix. Global AI Profiling Governance & International Cooperation

AI-driven profiling transcends national jurisdictions, making international cooperation essential to prevent regulatory fragmentation, ensure interoperability, and uphold consistent AI governance frameworks across borders. Japan must balance global alignment with its national strategic interests by engaging in multilateral efforts and reinforcing its leadership in AI governance. By reinforcing global AI leadership, ensuring data governance alignment, and harmonizing enforcement mechanisms, Japan can build a regulatory framework that safeguards domestic interests while remaining a key player in international AI governance.

- **Leading & Aligning with Global AI Standards:** Japan has played a pivotal role in shaping international AI regulation, particularly through the G7 Hiroshima AI Process, the OECD AI Principles, and ongoing collaboration with the EU AI Act framework. As AI governance continues to evolve, Japan could:
  - Strengthen engagement with **multilateral AI regulatory initiatives**, ensuring that its domestic policies remain interoperable with global standards.
  - Advocate for **risk-based, innovation-friendly AI governance**, balancing fundamental rights protections with economic and technological growth.
- **Data Sovereignty & The AI Data Supply Chain**: AI-driven profiling relies on large-scale cross-border data flows, creating a complex data supply chain that must balance national sovereignty with global economic integration. Japan could:
  - **Ensure regulatory clarity** on how foreign and domestic firms handle data generated in Japan, preventing unregulated data extraction while maintaining an open and innovation-driven digital economy.
  - **Promote structured international data-sharing agreements** that safeguard privacy, security, and compliance with domestic laws while allowing businesses to access global AI training datasets.
  - **Develop protocols for AI-driven cross-border data governance**, ensuring fair and lawful access to training data, compliance with privacy frameworks, and safeguards against misuse.
- **Harmonized Cross-Border Enforcement & Risk Detection:** As AI-driven profiling enables **global-scale market influence and potential risks**, regulatory enforcement cannot remain purely national. Japan could:
  - **Enhance cooperation between international enforcement agencies** to monitor AI-profiling abuses, algorithmic bias, and opaque decision-making at the cross-border level.
  - **Participate in joint AI risk assessments,** sharing best practices with global partners to detect and mitigate systemic AI-driven threats, such as misinformation, election manipulation, or discriminatory profiling.

- **Establish mechanisms for interoperability in compliance requirements**, allowing AI-driven firms to operate across jurisdictions without conflicting legal obligations or regulatory loopholes.

5. Conclusion

AI-driven profiling is reshaping digital interactions, influencing economic markets, social structures, and political processes in increasingly complex ways. While these technologies offer significant opportunities—enhancing consumer personalization, optimizing business operations, and improving public services—they also present substantial risks, including privacy erosion, bias reinforcement, exploitative practices, and threats to democratic integrity.

The EU's regulatory approach provides a structured model for balancing technological advancement with fundamental rights. Its emphasis on a risk-based framework, enforceable consumer protections, and corporate accountability, offers key insights for Japan as it refines its AI governance strategy.

This report outlines both **foundational considerations** and **regulatory recommendations** for Japan's effective development of an AI-profiling framework that is adaptive, rights-based, and forward-looking. Foundational considerations focus on ensuring that AI profiling regulation balances economic growth, innovation, and individual rights; establishes tiered, risk-and-dominance based compliance structures; promotes fairness in public and private profiling practices; prevents data monopolization; and encourages international regulatory alignment. Meanwhile, the recommendations provide a roadmap for structuring governance around enforceable rights, actionable transparency, sector-specific protections, responsible data-sharing frameworks that unlock the data economy, and agile regulatory processes to keep pace with technological developments.

As Japan refines its AI-profiling regulations, it must ensure that governance mechanisms serve innovation, economic progress, and individual autonomy. Profiling and algorithmic decision-making should not reinforce asymmetrical power dynamics between corporations, governments, and citizens but should instead be structured to promote fairness, competitiveness, and public trust.

By proactively shaping a regulatory framework that integrates economic opportunity with robust safeguards, Japan can strengthen its position as a global leader in AI governance—ensuring that AI-driven personalization aligns with societal values, safeguards fundamental rights, and fosters a competitive yet responsible economy.

Annex 1

Documents Analyzed & Key Findings

Document	Key Findings	Impact on AI Profiling
1. General Data Protection Regulation (GDPR)	Establishes a comprehensive data protection framework within the EU, requiring organizations to process personal data lawfully, fairly, and transparently. Introduces principles such as data minimization, purpose limitation, and accountability. Strengthens individual rights over personal data, including the right to access, rectify, erase, and restrict processing. Requires impact assessments for high-risk data processing activities and imposes strict obligations on data controllers and processors.	Regulates AI-driven profiling by imposing transparency requirements and granting individuals rights to access, rectify, and contest profiling-based decisions. Heightens requirements with regards to special categories of data, such as biometrics, racial or ethnic origin, or political opinions. Restricts fully automated decision-making when it produces legal or significant effects, unless specific conditions are met (e.g., explicit consent, legal authorization, or contractual necessity).
2. AI Act (Artificial Intelligence Act)	Establishes a risk-based regulatory framework for AI systems, categorizing them based on their potential societal impact. Introduces compliance obligations for AI systems deemed high-risk, including transparency, accountability, and oversight requirements. The level of regulatory scrutiny scales with the associated risk—higher-risk applications face stricter requirements, such as mandatory risk assessments, documentation, and continuous monitoring—while prohibiting AI applications that pose an unacceptable risk to fundamental rights.	Imposes restrictions on AI-driven profiling, with heightened requirements for high-risk systems. These requirements include pre-deployment risk assessments, bias mitigation strategies, human oversight, and continuous monitoring to ensure compliance with fundamental rights. High-risk AI profiling techniques include those used in hiring, credit scoring, law enforcement, and essential public services. Additionally, the Act prohibits certain profiling practices, including social scoring, exploitative targeting of vulnerable groups, and AI systems designed to manipulate behavior in ways that undermine autonomy.

Document	Key Findings	Impact on AI Profiling
3. Digital Services Act (DSA)	Requires transparency in algorithmic decision-making, particularly for very large online platforms and search engines, and mandates accountability in online platforms' content curation and advertising.	Mandates transparency in recommender systems, content ranking, and advertising, affecting AI-driven personalization and algorithmic decision-making.
4. Digital Markets Act (DMA)	Regulates large digital platforms (gatekeepers), ensuring fair competition, data-sharing obligations, and restrictions on anti-competitive behavior.	Prevents monopolistic AI profiling by dominant digital platforms, requiring fair data access and reducing anti-competitive profiling practices.
5. Right-to-Repair Directive	Strengthens consumer rights by ensuring access to repair information, spare parts, and independent repair services, with implications for digital products.	Influences digital product design by ensuring consumer rights to modify and repair AI-integrated products, impacting long-term data usage models, and governs over repair data.
6. Unfair Commercial Practices Directive	Targets misleading and aggressive commercial practices, including deceptive personalization and consumer manipulation techniques.	Mitigates AI-based deceptive personalization and manipulative consumer profiling, particularly in advertising and e-commerce contexts.
7. Data Act	Regulates data-sharing frameworks between businesses and consumers, establishing obligations on fair and non-discriminatory access to data.	Establishes frameworks for fair and non-discriminatory AI-driven data-sharing practices, addressing potential risks of market concentration and exploitation.
8. Commission Staff Working Document: Fitness Check of EU Consumer Law on Digital Fairness	Evaluates consumer protection laws for AI-driven personalization and profiling risks, identifying regulatory gaps in digital fairness and automated decision-making.	Identifies AI-specific consumer law gaps, particularly in algorithmic decision-making, AI-driven personalization, and voids in transparency obligations.

Annex 2

1. Foundational Considerations

Consideration Category	Description
1. Balancing Competing Priorities	Harmonizing AI innovation with economic interests and fundamental rights.
2. Building Trust Across Stakeholders	Ensuring trust among industry, individuals, and public institutions in AI governance.
3. Regulating Profiling Across Public and Private Sectors	Applying AI profiling regulations across private and public sector use.
4. Economic Growth, Social Equity, and Political Integrity	Aligning AI profiling policies with economic, social, and democratic values.
5. Corporate Accountability and Individual Rights	Holding corporations accountable while safeguarding individual freedoms.
6. Ensuring Regulatory Implementation	Moving beyond principles to enforceable AI profiling regulations with effective and efficient compliance mechanisms.
7. Managing Data Economy Risks and Opportunities	Recognizing AI-driven data markets' risks and ensuring fair opportunities.
8. Global AI and Data Governance Cooperation	Strengthening Japan’s engagement in global AI governance standards.
9. Addressing Data Asymmetries	Reducing AI-powered data monopolies and empowering individual rights.
10. Sector-Specific Protections & Compliance	Implementing differentiated AI compliance measures across industries.
11. Regulatory Agility and Adaptability	Designing adaptable, flexible, and responsive AI governance frameworks for evolving technology.

2. Regulatory Recommendations

Recommendation Category	Description
1. A Rights-Based Approach to AI Profiling	Establish enforceable rights for individuals to manage, challenge, and opt out of AI profiling.
2. Special Protections for Sensitive Data & Vulnerable Populations	Implement strict safeguards for sensitive data and protect vulnerable populations from exploitation.
3. Tiered Compliance for Agility & Risk Management	Apply proportional regulatory burdens based on risk and socioeconomic impact, ensuring fairness without stifling innovation.
4. Strengthening Individual Control Over Data	Ensure users can access, manage, and contest AI-driven decisions affecting them.
5. Enhancing & Protecting the Data Sharing Economy	Foster innovation and economic growth by enabling responsible data use while preventing monopolistic control, ensuring interoperability, and allowing government access to necessary data with strict safeguards to prevent overreach.
6. Preventing Manipulative AI Practices & Dark Patterns	Prohibit deceptive AI-driven personalization techniques that manipulate consumer behavior.
7. Compliance Throughout the AI Lifecycle	Implement lifecycle oversight structures, including pre-market certification, iterative auditing, and adaptive oversight mechanisms.
8. Robust Enforcement & Accountability	Ensure effective, proportionate, and dynamic enforcement of AI regulations.
9. Global AI Profiling Governance & International Cooperation	Align AI governance with international frameworks while maintaining robust national regulatory standards.