(Original version – September 2024)

Data Protection Authority of Belgium

General Secretariat

Artificial Intelligence Systems and the GDPR
A Data Protection Perspective

Executive summary

This information brochure outlines the complex interplay between the General Data Protection Regulation (GDPR)[i] and the Artificial Intelligence (AI) Act[ii] in the context of AI system development. The document emphasizes the importance of aligning AI systems with data protection principles while addressing the unique challenges posed by AI technologies.

Key points include:

- GDPR and AI Act alignment: the brochure highlights the complementary nature of the GDPR and AI Act in ensuring lawful, fair, and transparent processing of personal data in AI systems.
- AI system definition: the document provides a clear definition of AI systems and offers illustrative examples to clarify the concept.
- data protection principles: the brochure delves into core GDPR principles such as lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, and data subject rights in the context of AI systems.
- accountability: the importance of accountability is emphasized, with specific requirements outlined for both the GDPR and AI Act.
- security: the document highlights the need for robust technical and organizational measures, to protect personal data processed by AI systems.
- human oversight: The crucial role of human oversight in AI system development and operation is emphasized, particularly for high-risk AI systems.

By providing insights into the legal framework and practical guidance, this information brochure aims to empower legal professionals, data protection officers, technical stakeholders, including controllers and processors, to understand and comply with the GDPR and AI Act requirements when developing and deploying AI systems.

Objective of this information brochure

The General Secretariat of the Belgian Data Protection Authority monitors social, economic, and technological developments that impact the protection of personal data[iii].

In recent years, AI technologies have experienced exponential growth, revolutionizing various industries and significantly impacting the way data is collected, processed, and utilized. However, this rapid advancement has brought about complex challenges regarding data privacy, transparency, and accountability.

In this context, the General Secretariat of the Belgian Data Protection Authority publishes this information brochure to provide insights on data protection and the development and implementation of AI systems.

Understanding and adhering to the GDPR principles and provisions is crucial for ensuring that AI systems operate ethically, responsibly, and in compliance with legal standards. This information brochure aims to elucidate the GDPR requirements specifically applicable to AI systems, offering more clarity and useful insights to stakeholders involved in the development, implementation, and (internal) regulation of AI technologies.

In addition to the GDPR, the Artificial Intelligence Act (AI Act), which entered into force on 1st of August 2024, will also significantly impact the regulation of AI system development and use. This information brochure will also address the requirements of the AI Act.

Audience for this information brochure

This information brochure is intended for a diverse audience comprising legal professionals, Data Protection Officers (DPOs), and individuals with technical backgrounds including business analysts, architects, and developers. It also targets controllers and processors involved in the development and deployment of AI systems. Given the intersection of legal and technical considerations inherent in the application of the GDPR to AI systems, this information brochure seeks to bridge the gap between legal requirements and technical implementation.

Legal professionals and DPOs play a crucial role in ensuring organizational compliance with GDPR obligations, specifically those relevant to AI systems that process personal data. By providing insights into GDPR requirements specific to AI, this information brochure equips legal professionals and DPOs with useful knowledge to navigate the complexities of AI-related data processing activities, assess risks, and implement appropriate measures.

At the same time, individuals with technical backgrounds such as business analysts, architects, and developers are integral to the design, development, and deployment of AI systems. Recognizing their pivotal role, this information brochure aims to elucidate GDPR requirements in a manner accessible to technical stakeholders. Concrete, real-life examples are incorporated into the text to illustrate how GDPR principles translate into practical considerations during the lifecycle of AI projects. By offering actionable insights, this information brochure empowers technical professionals to design AI systems that are compliant with GDPR obligations, embed data protection-by-design principles, and mitigate potential legal and ethical risks.

What is an AI system ?

The term "AI system" encompasses a wide range of interpretations.

This information brochure will not delve into the intricacies and nuances that distinguish these various definitions.
Instead, we will begin by examining the definition of an AI system as outlined in the AI Act[iv]:

For the purposes of this Regulation, the following definitions apply:
(1) 'AI system' means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments;

In other terms :
An AI system is a computer system specifically designed to analyze data, identify patterns, and use that knowledge to make informed decisions or predictions.
In some cases, AI systems can learn from data and adapt over time. This learning capability allows them to improve their performance, identify complex patterns across different data sets, and make more accurate or nuanced decisions.

Examples of AI systems in everyday life:

Spam filters in email: spam filters analyze incoming emails and identify patterns that distinguish spam messages from legitimate emails. Over time, as people mark emails as spam or not spam, the AI system can learn and improve its filtering accuracy. This is an example of an AI system that meets the criteria of an AI system :

- machine-based system: it's a computer program.
- analyzes data: it analyzes the content of emails.
- identifies patterns: it identifies patterns in emails that suggest spam.
- makes decisions: it decides whether to categorize an email as spam or not.

Recommendation systems on streaming services: movie streaming services utilize AI systems to generate recommendations for users. These systems analyze a user's past viewing habits, along with the habits of similar users, to recommend content they might be interested in. This is another example of an AI system :

- machine-based system: it's a computer program.
- analyzes data: it analyzes a user's viewing/listening history.
- identifies patterns: it identifies patterns in user preferences and those of similar users.
- makes recommendations: it recommends content based on the identified patterns.

Virtual assistants: virtual assistants respond to voice commands and complete tasks like setting alarms, playing music, or controlling smart home devices. These systems use speech recognition and natural language processing to understand user requests and take action. This is again an example of an AI system :

- machine-based system: it's a computer program.
- analyzes data: it analyzes user voice commands.
- identifies patterns: it identifies patterns in speech to understand user requests.
- makes decisions: it decides how to respond to commands based on its understanding.
- may exhibit adaptiveness: some virtual assistants can learn user preferences and adapt their responses over time.

AI-powered medical imaging analysis: many hospitals and healthcare providers are utilizing AI systems to assist doctors in analyzing medical images, such as X-rays, CT scans, and MRIs. These systems are trained on vast datasets of labeled medical images, allowing them to identify patterns and potential abnormalities.

- machine-based system: it's a computer program.
- analyzes data: it analyzes the digital medical images.
- identifies patterns: it identifies patterns in the images that might indicate the presence of a disease or abnormality.
- supports decision-making: the system highlights potential areas of concern in the images, which can help doctors make more informed diagnoses.

GDPR & AI Act requirements

Lawful, fair, and transparent processing

The GDPR requires lawfulness, fairness and transparency.

Leveraging GDPR lawfulness of processing: The GDPR establishes six legal bases for processing personal data in Article 6 (consent, contract, legal obligation, vital interests, public interest, and legitimate interests). These same legal bases remain applicable for AI systems that process personal data under the AI Act.

Prohibited AI Systems: the AI Act introduces additional prohibitions beyond the GDPR for certain high-risk AI systems. While the GDPR focuses on protecting personal data through various principles, the AI Act directly prohibits specific types of high-risk AI applications. Here are some examples:

- Social scoring systems: these systems assign a score to individuals based on various factors, potentially leading to discrimination and limitations on opportunities.
- AI systems for real-time facial recognition in public places (with limited exceptions): these systems raise concerns about privacy, freedom of movement, and potential misuse for mass surveillance.

Fairness:

- While the AI Act doesn't have a dedicated section titled “fairness”, it builds upon the GDPR's principle of fair processing (art. 5.1.a) as the AI Act focuses on mitigating bias and discrimination in the development, deployment, and use of AI systems.

Transparency:

- the AI Act requires a baseline level of transparency for all AI systems. This means users should be informed that they're interacting with an AI system. For instance, a chatbot could begin an interaction with a message like "Hello, I am Nelson, **a chatbot**. How can I assist you today?"
- the AI Act requires a higher transparency level for high-risk AI systems. This includes providing clear and accessible information about how data is used in these systems, particularly regarding the decision-making process. Users should understand the factors influencing AI-based decisions and how potential bias is mitigated.

Purpose limitation and data minimisation

The GDPR requires purpose limitation (art. 5.1.b) and data minimisation (art. 5.1.c). This means personal data must be collected for specific and legitimate purposes, and limited to what is necessary for those purposes. These principles ensure that AI systems don't use data for purposes beyond their intended function or collect excessive data.
The AI Act strengthens the principle of purpose limitation – from the GDPR – for high-risk AI systems by emphasizing the need for a well-defined and documented intended purpose.

Example : A loan approval AI system of a financial institution, in addition to standard identification data and credit bureau information, also utilizes geolocation data (e.g., past locations visited) and social media data (e.g., friends' profiles and interests) of a data subject. This extensive data collection, including geolocation and social media data, raises concerns about the system's compliance with the GDPR.

Data accuracy and up-to-dateness

The GDPR requires personal data to be accurate and, where necessary, kept up-to-date (art. 5.1.d). Organizations must take reasonable steps to ensure this. The AI Act builds upon this principle by requiring high-risk AI systems to use high-quality and unbiased data to prevent discriminatory outcomes.

Example : a financial institution develops an AI system to automate loan approvals. The system analyzes various data points about loan applicants, including credit history, income, and demographics (postal code). However, the training data for the AI system unknowingly reflects historical biases : the data stems from a period when loans were more readily granted in wealthier neighborhoods (with a higher average income). The AI system perpetuates these biases as loan applicants from lower-income neighborhoods might be systematically denied loans, even if they are financially qualified. This results in a discriminatory outcome, and might raise serious concerns about the system's compliance with the AI Act.

Storage limitation

The GDPR requires personal data to be stored only for as long as necessary to achieve the purposes for which it was collected (art. 5.1.e). The AI Act doesn't explicitly introduce another or an extra requirement on storage limitation for high-risk AI systems.

Automated decision-making

The GDPR and the AI Act both address the importance of human involvement in automated decision-making processes that impact individuals. However, they differ in their focus:

- The GDPR grants individuals the right not to be subject solely to automated processing for decisions that produce legal effects concerning them (art. 22). This means data subjects have the right to request a reconsideration of an automated decision by a human decision-maker. This functions as an individual right to challenge decisions perceived as unfair or inaccurate.
- The AI Act strengthens the focus on human involvement by requiring meaningful human oversight throughout the development, deployment, and use of high-risk AI systems. This acts as a governance measure to ensure responsible AI development and use. Human oversight under the AI Act encompasses a broader range of activities than just reconsideration of individual decisions. It includes, for example, reviewing the AI system's training data and algorithms for potential biases, monitoring the system's performance, and intervening in critical decision-making pathways.

In essence, the GDPR empowers individuals to object to solely automated decisions, while the AI Act requires proactive human oversight for high-risk AI systems to safeguard against potential biases and ensure responsible development and use of such systems.

Example : a government agency uses an AI system to assess eligibility for social welfare benefits based on income, employment status, and family situation.
Following the GDPR, individuals have the right not to be subject solely to automated processing for social welfare benefits eligibility (art. 22). This means they can request a reconsideration of an automated decision by a human decision-maker.
Following the AI Act, this AI system is classified as an high-risk system (as it has a significant impact on individuals' livelihoods). This requires the government agency to implement human oversight throughout the development, deployment, and use of the AI system.

Security of Processing

Both the GDPR and the AI Act emphasize the importance of securing personal data throughout its processing lifecycle. However, AI systems introduce specific risks that require additional security measures beyond traditional data protection practices.

The GDPR requires organizations to implement technical and organizational measures (TOMs) that are appropriate to the risk associated with their data processing activities. This involves conducting risk assessments to identify potential threats and vulnerabilities. The selected TOMs should mitigate these risks and ensure a baseline level of security for personal data.

The AI Act builds upon this foundation by mandating robust security measures for high-risk AI systems. This is because AI systems introduce specific risks that go beyond traditional data processing, such as:

- potential bias in training data: biased training data can lead to biased decisions by the AI system, impacting individuals unfairly.
- manipulation by unauthorized individuals: for example, a hacker could potentially manipulate the AI system's training data to influence its decisions in a harmful way. Imagine a system trained to approve loan applications being tricked into rejecting qualified applicants based on irrelevant factors.

To address these unique risks, the AI Act emphasizes proactive measures such as:

- identifying and planning for potential problems: This involves brainstorming what could go wrong with the AI system and how likely it is to happen (risk assessment). This is a core practice under both the GDPR and AI Act.
- continuous monitoring and testing: This involves regularly evaluating the AI system's performance for several aspects including:
    - security flaws: identifying vulnerabilities in the system's code or design that could be exploited by attackers.
    - bias: checking for potential biases in the system's training data or decision-making processes.
- human oversight: the AI Act emphasizes the importance of meaningful human oversight throughout the development, deployment, and use of high-risk AI systems. This ensures that humans are involved in critical decisions and

understand the system's vulnerabilities. Human oversight under the AI Act goes beyond just security processes and encompasses various aspects, such as:

- reviewing training data and algorithms for potential biases.
- monitoring the system's performance for fairness, accuracy, and potential unintended behaviour.
- intervening in critical decision-making pathways, especially when they could significantly impact individuals.

Example: AI-powered Lung Cancer Diagnosis System.

An AI system used by a hospital to diagnose lung cancer exemplifies a high-risk AI system due to several factors:

- highly sensitive data: it processes highly sensitive personal data, including patients' health information (lungs) and diagnoses (special category data under article 9 of the GDPR) ;
- data breach impact: a data breach could expose critical health information about patients, potentially leading to privacy violations and reputational harm for the hospital ;
- life-altering decisions: the system's output directly impacts patients' lives. A diagnosis based on inaccurate or compromised data could have serious consequences for their health and well-being.

Both the GDPR and the AI Act emphasize the importance of security measures for data processing activities, especially those involving sensitive data.

- the GDPR establishes a foundation for data security: It requires organizations to implement appropriate technical and organizational measures (TOMs) to protect personal data based on a risk assessment. For health data, these measures would be particularly strong due to its sensitive nature. Examples under the GDPR could include:
  - data encryption: encrypting patient data at rest and in transit ensures its confidentiality even if a breach occurs ;
  - access controls: implementing strict access controls limits who can access and modify patient data ;
  - penetration testing: regularly conducting penetration tests helps identify and address vulnerabilities in the system's security posture ;
  - logging and auditing: maintaining detailed logs of system activity allows for monitoring and investigation of any suspicious behavior.
- The AI Act builds upon this foundation for high-risk AI systems: recognizing the specific risks of AI, the AI Act mandates robust security measures. These might

include additional measures tailored to the specific vulnerabilities of the AI system, such as data validation and quality assurance : the AI Act emphasizes the importance of ensuring the quality and integrity of the data used to train and operate the AI system. This could involve techniques for:

- data provenance: tracking the origin of data to identify potential sources of bias or manipulation in the training data, such as incorrect X-ray labeling.
- anomaly detection: identifying and flagging unusual patterns in the training data that might indicate malicious tampering, such as a sudden influx of X-rays with unrealistic characteristics.
- human review of high-risk data points: Having healthcare professionals review critical X-rays before they are used to train the AI system, especially those that show unusual features or could significantly impact patient outcomes.

By implementing these security measures the hospital can mitigate the risks associated with the AI-powered lung cancer diagnosis system and ensure patient privacy, data security, and ultimately, the best possible patient outcomes.

Data Subject Rights

The GDPR grants natural persons data subject rights, empowering them to control their personal data and how it's used. These rights include access (seeing what data is processed, art. 15), rectification (correcting inaccurate data and completing data, art. 16), erasure (requesting data deletion, art. 17), restriction of processing (limiting how data is used, art. 18), and data portability (transferring data to another service, art. 20).

To effectively exercise these rights, natural persons need to understand how their data is being processed. The AI Act reinforces this by emphasizing the importance of clear explanations about how data is used in AI systems. With this transparency, individuals can make informed decisions about their data and utilize their data subject rights more effectively.

Example : an AI system used to determine car insurance premiums assigns a relatively high premium to a particular customer (data subject). The AI Act entitles this customer to a clear explanation of how their premium is calculated. For example, the insurer (data controller) could explain that various data points were used, such as the customer's annual mileage, accident history, and whether the car is used for work purposes. This information, in turn, allows the customer to exercise their data subject rights under the GDPR, such as the right to rectification (correction of inaccurate personal data or completion of personal data).

Accountability

The GDPR requires (organizations to demonstrate) accountability for personal data processing through several measures, such as :

- Transparent processing: individuals must understand how their data is collected, used, stored and shared (f.e. by a clear and concise data protection statement, by data subject access rights, …). This transparency allows them to see if their data is being handled lawfully and fairly ;
- Policies and procedures for handling personal data: documented policies ensure consistent data handling practices across the organization ;
- Documented legal basis for processing: for each data processing activity, organizations need documented proof of the lawful justification (consent, contract, legitimate interest, etc.) ;
- Keeping different records (like the Register Of Processing Activities (ROPA), data subject requests, data breaches) is required: maintaining accurate records demonstrates a commitment to accountability and allows organizations to prove compliance during audits or investigations ;
- Security measures: implementing and correctly maintaining appropriate technical and organizational measures (TOMs) to protect personal data is crucial for demonstrating accountability ;
- A Data Protection Impact Assessment (DPIAs) is required in some cases: these are mandatory when processing high-risk data or implementing new technologies ;
- A Data Protection Officer (DPO) is required in some cases: f.e. governmental organizations, regardless of their core activities, are required to have a DPO.

While the AI Act doesn't have a dedicated section on demonstrating accountability, it builds upon the GDPR's principles. The AI Act requires organizations to implement :

- a two-step risk management approach for AI systems. First, there's an initial classification process that categorizes the risk the AI poses to individuals (ranging from minimal to high).
  For high-risk systems, a more in-depth risk assessment is required. This dives deeper into the specific risks and identifies potential harms associated with the AI system, and is also called a FRIA (Fundamental Rights Impact Assessment) ;
- clear documentation of the design and implementation of AI systems ;

- processes dealing with human oversight in high-risk AI systems. This could involve human intervention or approval for critical decisions made by the AI system ;
- a formal incident reporting process for reporting incidents related to AI system malfunctions or unintended behaviour.

Making compliance straightforward: user stories for AI systems in light of GDPR and AI Act requirements

Translating regulatory requirements into technical specifications for AI systems presents significant challenges. This document focuses on using user stories to bridge the gap between legal obligations and system development.

User stories offer a practical approach to understanding and addressing regulatory requirements in the context of AI system design. By adopting a user-centric perspective, organizations can effectively translate legal obligations into actionable steps.

This document uses a car insurance premium calculation system as an example to illustrate the application of user stories in the AI domain.

Requirements of lawful, fair, and transparent processing

User story: ensuring lawfulness – correct legal basis

As a car insurance company implementing an AI system for car premium calculations, we need to conduct a thorough legal basis assessment to determine the most appropriate legal justification for collecting and using customer data in our AI system. This is important to comply with the GDPR principle of lawfulness.

***User story:* ensuring lawfulness - prohibited data**

As a car insurance company implementing an AI system for car premium calculations, we need to ensure our system complies with the GDPR and AI Act prohibitions on processing certain types of personal data. This includes special categories of personal data such as racial or ethnic origin, political opinions, religious beliefs, etc. This is important to comply with the GDPR's protection of sensitive personal data and the AI Act's emphasis on preventing discriminatory outcomes.

User story: ensuring fairness

As a car insurance company implementing an AI system for car premium calculations, we need to ensure fair and non-discriminatory processing of customer data. This is important to comply with the GDPR principle of fairness and the specific AI Act's focus on preventing biased outcomes that could disadvantage certain groups.

The car insurance company can achieve fairness by:

- data source review: analyze the data sources used to train the AI system to identify and mitigate potential biases based on factors like postal code, gender, age, … . Ensure these factors are used in a way that is relevant and necessary for premium calculations, avoiding any discriminatory outcomes.
- fairness testing: regularly test the AI system for potential biases in its outputs. This might involve comparing car premium calculations for similar customer profiles to identify any unexplainable disparities.
- human oversight: implement a human review process for high-impact decisions made by the AI system, such as significant car premium increases or even policy denials.

User story: ensuring transparency

As a car insurance company implementing an AI system for car premium calculations, we need to be transparent about how our customers' data is used. This is important to comply with the general GDPR principle of transparency and the specific AI Act's focus on transparency for high-risk AI systems.

The car insurance company can achieve transparency by :

- a data protection statement : clearly explain in the company's data protection statement how customer data is collected, used, and stored in the AI system for premium calculations.
- easy-to-understand explanations : provide customer-friendly explanations of the AI premium calculations process. This could involve using simple language, visuals, or FAQs to demystify the AI's role in determining car insurance premiums.
- right to access information : implement mechanisms for customers to easily access information about the data points used in their specific premium calculations.

Requirements of purpose limitation and data minimization

User story : ensuring purpose limitation

As a car insurance company implementing an AI system for car premium calculations, we need to ensure that the data we collect from our customers is limited to what is strictly necessary for the accurate premium calculations. This is important to comply with the principle of purpose limitation under the GDPR.

User story : ensuring data minimization

As a car insurance company implementing an AI system for car premium calculations, we need to implement a data minimization strategy to ensure we only collect and use the minimum amount of customer data necessary for the accurate premium calculations. This is important to comply with the principle of data minimization under the GDPR.

Requirements of data accuracy and up-to-dateness

User story : ensuring data accuracy and up-to-dateness

As a car insurance company implementing an AI system for car premium calculations, we need to implement processes to ensure the accuracy and up-to-dateness of customer data used in the system. This is important to comply with the principle of data accuracy under the GDPR.

The car insurance company can achieve accuracy and up-to-dateness of customer data by:

- data verification mechanisms: offer customers easy-to-use mechanisms to verify and update their personal data within the car insurance system. This could be through an online portal, mobile app, or dedicated phone line.
- regular data refresh: establish procedures for regularly refreshing customer data used in the AI system. This might involve requesting customers to update their information periodically or integrating with external data sources (e.g., driving record databases) to automatically update relevant data points.
- data quality alerts: implement alerts for missing or potentially inaccurate data points in customer profiles. This allows the company to proactively reach out to customers and request updates.
- clearly communicate to customers their right to rectification under the GDPR. This right allows them to request corrections of any inaccurate personal data or completion of missing data used in the premium calculations system.

User story : ensuring use of unbiased data

As a car insurance company implementing an AI system for car premium calculations, we need to ensure that the data used to train and operate the system is of free from bias. This is important to comply with the specific AI Act's focus on preventing biased outcomes that could disadvantage certain groups.

The car insurance company can achieve unbiased data for fair AI premium calculations by :

- data source evaluation: Analyze the sources of data used to train the AI system. Identify potential biases based on factors like socioeconomic background in the data collection process.
- regular monitoring and bias testing: Continuously monitor the AI system's performance for potential biases in its outputs. Conduct regular bias testing to identify and address any discriminatory outcomes in premium calculations.
- human oversight: implement a human review process for high-impact decisions made by the AI system, such as significant car premium increases or even policy denials. This allows human intervention to prevent biased out comes.
- transparency with customers: Inform customers in the data protection statement about the company's commitment to using high-quality, unbiased data in the AI system.

Requirement of secure processing

User story : implementing appropriate security measures for car insurance AI

As a car insurance company implementing an AI system for car premium calculations, we need to conduct a thorough risk assessment to identify potential threats and vulnerabilities that could impact our customer data. This assessment will consider various factors, including the type of data (financial data vs. basic customer information), processing activities, and potential impact of a security breach. Based on this assessment, we will implement appropriate technical and organizational measures (TOMs) to mitigate these risks and ensure the security of our customer data. This is important to comply with the requirement of security of the processing under the GDPR.

Examples of TOMs may include:

- data encryption: encrypting customer data at rest and in transit to protect confidentiality ;
- access controls: implementing strict access controls to limit who can access and modify customer data ;
- regular penetration testing: conducting penetration tests to identify and address vulnerabilities in the system's security posture ;
- logging and auditing: maintaining detailed logs of system activity for monitoring and investigation of any suspicious behavior.

User story : implementing specific security measures for car insurance AI

As a car insurance company implementing an AI system for car premium calculations, we recognize that AI systems introduce specific risks beyond traditional data processing. These risks might include potential bias in training data or manipulation by unauthorized actors. To address these specific risks we will implement additional measures in conjunction with the baseline GDPR-compliant TOMs. This is important to comply with the requirement of security of the processing under the AI Act.

Examples of these additional measures may include:

- data validation and quality assurance: implementing processes to ensure the quality and integrity of the data used to train and operate the AI system. This could involve data provenance tracking and anomaly detection to identify potential biases or manipulation attempts.
- human oversight: establishing a framework for human oversight throughout the AI system's lifecycle. This could involve human review of high-risk data points, monitoring the system's performance for fairness and accuracy, and intervening in critical decision-making pathways.

Requirement of (the ability of demonstrating) accountability

User story : documenting the legal basis

As a car insurance company implementing an AI system for car premium calculations, we need to have a clear and concise record of the legal basis for collecting and using customer data in the AI system. This is important to comply with the GDPR principle of (demonstrating) accountability (also in the context of audits or investigations).

User story : conducting a Fundamental Rights Impact Assessment (FRIA)

As a car insurance company implementing an AI system for car premium calculations, we need to develop and maintain a comprehensive FRIA (Fundamental Rights Impact Assessment) to proactively identify and mitigate potential risks associated with this AI system. This is important to comply with the AI Act's requirements for high-risk AI systems and promote fair and non-discriminatory premium calculations for our customers.

* * *

References

[0] This paper also utilized spelling and grammar checking, and a large language model, as a tool for refining and correcting initial text sections.
[i] Regulation (EU)2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the European Union L 119/1, 4.5.2016, p. 1–88.
[ii] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), Official Journal of the European Union L 199/1, 12.7.2024, p. 1–120.
[iii] Art. 20, §1, 1°, Data Protection Authority Act of 3 December 2017, amended by the Act of 25 December 2023.
[iv] Artificial Intelligence Act, Article 3 (1)