(Original version – version April 2026)

Data Protection Authority of Belgium

The impact of artificial intelligence on privacy

Table of contents

Objective of this information brochure

The Belgian Data Protection Authority (Belgian DPA) continuously monitors social, economic, and technological developments that affect the protection of personal data.

Among these evolving trends, the use of Artificial Intelligence (AI) systems has expanded beyond industry and academia into the daily life of citizens. From virtual assistants' tools to AI-assisted medical diagnosis, individuals are increasingly interacting with AI systems. Some of these systems are trained on personal data[1] collected from various sources, including social media feed, internet queries, inputs in chatbots, or online purchases. However, the complexity and opaqueness of AI systems make it difficult to understand the personal data being gathered, the purpose of processing[2], or the way decisions are taken. These characteristics affect individuals' exercise of their right to data protection, resulting in a loss of control over personal data and limiting their capacity to challenge unfair outcomes.

The rights to privacy and data protection, enshrined in the Charter of Fundamental Rights of the European Union and the General Data Protection Regulation (GDPR), provide for objective rights aimed at ensuring individual's control over their personal data. In addition, the Artificial Intelligence Act (AI Act) sets up a regulatory framework for the development and deployment of AI systems aimed at fostering an innovative environment while respecting individuals' safety, health and fundamental rights.

In this context, this information brochure has been prepared to help individuals understand how AI systems may affect their privacy and the protection of their personal data. It also provides practical recommendations to help individuals keep control over their data in an increasingly AI-driven environment.

Drawing on the scope of the "Artificial Intelligence Systems and the GDPR: A data protection perspective" brochure of December 2024, the General Secretariat intends to dive into specific topics to raise awareness among citizens, increase AI literacy, and give practical advice to the industry through a series of publications on AI and data protection. The full series can be explored **here**.

[1] Article 4(1) GDPR: "*'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;*"
Remark: Stricter protection apply for special categories of data (e.g., health, race, religion) processing under article 9 of the GDPR.
[2] Article 4(2) GDPR: " *'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;*"

Audience for this information brochure

This information brochure is intended for individuals who use or interact with AI systems in their daily lives – whether through online platforms, mobile applications, connected devices, or other digital services.

It is designed for readers who wish to understand how AI systems use their personal data and how this may affect their private life, without requiring a technical or legal background.

Through clear explanations and concrete examples, the brochure offers a concise overview of what AI systems are, how they work, the types of personal data they collect and process, the potential privacy risks involved, and the rights that individuals have under data protection law – along with simple steps to exercise those rights.

The impact of artificial intelligence on privacy

1. AI system

1.1. Notion and characteristics

The AI Act defines an AI system as: "*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*[3]*, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments*"[4].

This definition adopts a lifecycle-based perspective distinguishing AI system's development phase from their deployment. In that regard, it recognizes that their characteristics may appear in one phase without carrying over to the other.[i]

In essence, AI systems are computer-based systems that can make decisions by analysing data and identifying patterns. Their autonomy enables the learning from said data to adapt and improve performance in order to generate more accurate or nuanced outcomes, sometimes by inferring future behaviour.[ii]

1.2. AI system & AI model

What distinguishes AI systems from traditional automation systems – such as pre-defined customer segmentation (users grouped based on previously defined attributes) or fixed-rule data masking tools (replacing names or IDs with pseudonyms using fixed patterns) – is their ability to infer from data or knowledge.[iii] AI systems incorporate advanced data processing techniques[5] to infer from data and, in some cases, to learn or adapt.[iv]

These data processing techniques are carried out by one, or more, AI model(s) contained within an AI system. An AI model is an algorithm trained on a dataset to perform a set of tasks predefined or learned through training. AI systems integrate AI model(s) with other system components (monitoring tools, application programming interfaces [APIs], etc.).[v]

The Cooking analogy is helpful to grasp the difference. AI model training consists of the creation of a cake recipe, while the AI system bakes the cake. The baked cake (the output) depends on the quality of the ingredients (the data), the reliability of the recipe (the AI model architecture), and the steps to follow (the algorithm). The integration of that model into the AI system enables the cake to be baked by following the recipe, with the correct

[3] Explicit objectives are those intentionally encoded into the system by its developer (e.g., minimize error, maximize click-through rate, predict disease risk). Implicit objectives are inferred from the system's behaviour or underlying assumptions (e.g., favouring emotionally provocative posts, amplifying polarising content, or prioritising content from highly active users may indicate a hidden goal of increasing engagement).
[4] Article 3(1) of the AI Act.
[5] Two main approaches to data processing can be distinguished. On the one hand, with a machine learning approach, the AI system learns from the data how to achieve a specific set of objectives. On the other hand, with the logic- and knowledge-based approaches, AI systems have the ability to infer information from the encoded knowledge or symbolic representation of the tasks at hand.

ingredients, executing the steps in order, and using the oven, cake pan, mixing bowls, etc. (the infrastructure, APIs, interfaces, etc.) to complete the process.

1.3. AI system's application domains

AI systems can be used in many cases[6]. Therefore, depending on their aim, AI systems can be classified in one or more of the following categories. The aim for which an AI system is intended to be used will also help to identify the categories of data needed for its training and deployment.

Expert systems simulate the decision-making ability of a human expert in specific domains (e.g., providing automated clinical diagnostic comments on medical reports). They often require structured personal data such as health records, legal case histories, or diagnostic information.

Autonomous systems can operate independently in dynamic environments (e.g., self-driving cars, drones). They may process location data, sensor data, or biometric identifiers.

Cognitive computing mimics human thought processes to interpret unstructured data and support decision-making (e.g., systems used for evaluating patients' information). These systems often use diverse personal data such as e-mails, voice recordings, documents, and chat logs.

Computer vision interprets visual inputs, such as images or videos, for recognition, tracking or analysis tasks (e.g., systems used in monitoring patients' movements). Such system can process facial images, gait patterns, and video footage.

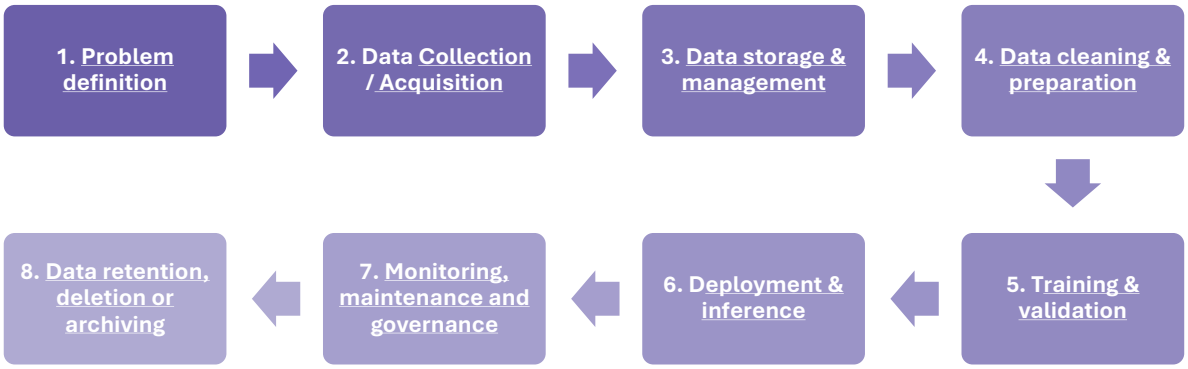
AI-powered robots relate to machines that perform complex tasks through interaction with their environment (e.g., autonomous robotic vacuum cleaners). Depending on their application, they may use audio-visual data and location data.

Natural language processing AI systems are designed to understand, interpret, and generate human language in text or speech form (e.g., chatbots). These systems often process chat histories, voice commands.

1.4. AI system's lifecycle and related data processing activities

Regardless of their aim, AI systems usually follow similar data processing activities during their lifecycle. The figure below show the data processing activities usually carried out throughout an AI system's lifecycle.

[6] See the brochure 'Artificial Intelligence Systems and the GDPR: A Data Protection Perspective', pages 6-7, published by the Data Protection Authority of Belgium.



vi

1. Problem definition: The first step consists in identifying the AI system's purpose. This purpose should be clearly defined and generally include objectives, success criteria, and regulatory obligations.

2. Data Collection/Acquisition: The second step entails the collection or acquisition of raw data, including personal data, from various sources. Such sources include, but are not limited to:

- Social media activity: Online posts, 'likes', comments, connections, etc.
- Customer databases: Names, e-mails, phone numbers, purchase history, etc.
- Transaction records: Credit-card payments, invoices, loyalty-card logs, etc.
- Browsing history: Visited websites, search queries, click patterns, etc.
- Public records: Company registries, property deeds, forum posts, etc.
- Smart devices: Voice commands, GPS location, fitness tracker metrics, etc.

3. Data storage and management: The third step is aimed at securely storing and managing the data collected or acquired in the previous step. This includes applying appropriate storage conditions and security measures such as encryption, access controls, and privacy-preserving mechanisms.

4. Data cleaning and preparation: In the fourth step, raw data is pre-processed to improve quality and consistency while ensuring privacy. These pre-processing activities may involve the correction of errors in the data (e.g., over or under representation of certain demographics), standardisation of the data (e.g., all dates are recorded under this format: DD/MM/YYYY; all gender data is recorded under this format: Male/Female), and when possible, the pseudonymisation or anonymisation of the personal data. Once the data is cleaned, it usually is split into three different datasets that will each serve their own purpose in the fifth step (training dataset, validation dataset, and the test dataset).

5. Training and validation: In this step, the datasets are used train, validate and test an AI system to ensure the accurate performance of the AI system. Validation data helps adjust the system during training while test data is used to assess key performance metrics such as accuracy, fairness, and generalisability. Training data is used to train the AI system previous to its deployment.

6. Deployment and inference: Following successful validation, a trained AI system is deployed and starts to receive input data (e.g., user prompts or system-generated queries) and generate outputs. Filtering mechanisms may be applied to avoid unwanted inputs or prohibited outputs.

7. Monitoring, maintenance and governance: After deployment, an AI system is monitored to ensure expected performance. Feedback and system data may be used for model fine-tuning or retraining. Governance processes ensure compliance, auditability, and accountability across the AI lifecycle.

8. Data retention, deletion or archiving: Personal data should be retained only as long as necessary. Once no longer needed, data must be securely deleted, anonymised, or archived in line with applicable data protection laws and organisational policies.

It is worth noting that the seventh and eighth steps can be carried out simultaneously and represent a continuous process. During an AI system's lifecycle, ongoing monitoring is necessary to identify unfair or inaccurate outcomes. This monitoring allows adaptation of the AI system to improve performance and correct inaccuracies – whether they stem from the training or validation data, or from the underlying source code.

2. Privacy risks

AI systems introduce new dimensions to privacy risks through extensive data collection and processing practices. These risks arise from illicit or unauthorized personal data collection, processing, or sharing. However, even lawful data practices can pose privacy concerns – particularly when they lack transparency, fairness, or proportionality – examples include excessive surveillance, profiling, or unforeseen secondary uses of data.

AI systems may scale up privacy risks – such as the risk of excessive or disproportionate data collection and potential breaches of the data minimisation principle (Article 5(1)(c) GDPR) – due to their ability to process vast amounts of personal data often in real time. Risks that were once isolated – such as manual profiling[7], limited surveillance, or targeted advertising – can now be transformed into systemic concerns. AI systems can be used to profile millions of users, apply facial recognition across public spaces, and deliver highly personalized and targeted advertisements.[vii] The speed, scale and opacity of AI systems' automated-decision making render privacy and data protection violations difficult to prevent.

AI-driven automation has the potential to remove or reduce human oversight from automated data-based decisions. Such automated assessments are used in everyday scenarios such as creditworthiness estimation, security risks evaluations, and recruitment or selection processes. This automated decision-making characteristic raises concerns about transparency and human involvement, which may undermine fair outcomes and

[7] Article 4(4) of the GDPR: "*'profiling' means 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;*".

restrict individuals' ability to seek redress.[viii] Although Article 22 of the GDPR prohibits decisions based solely on automated processing that produce significant effects (see section 3.2(h)), exemptions are provided under specific conditions and safeguards.

AI's ability to infer sensitive personal data can induce illegal processing activities or the categorization and profiling of citizens.[ix] Using machine learning techniques, AI systems can derive attributes such as sexual orientation, religious beliefs, health conditions, or emotional state from indirect sources like browsing history, online purchase history, or voice tone – often without the individual's knowledge or consent. In addition, inferences may be inaccurate or misleading due to their probabilistic[x] characteristic (statistical estimations rather than verified facts).

3. Protecting one's personal data

The GDPR has a large scope and covers activities involving the processing of personal data within the EU.[8] AI systems may process personal data at different steps of its lifecycle[xi], sometimes not purposefully. In fact, AI systems aimed at not processing personal data need to be trained to recognize personal data. In that case, personal data will be included in the training, validation and testing datasets hence personal data will be processed in the development phase.

Article 5 of the GDPR enumerates principles which all personal data processing activities must respect. These principles require that personal data must be: processed in a lawful, loyal and transparent manner; collected for a specified, explicit and legitimate purpose; adequate, relevant, and necessary to attain that purpose; accurate, and up to date; stored no longer than necessary for the processing operation; and, appropriately secured. In addition, controllers[9] must be able to demonstrate compliance with these principles.

From the transparency principle, controllers are obliged to inform individuals about the processing activities in a clear and accessible manner. More specifically and when applicable, controllers may have to elaborate on the logic underpinning automated decision making, such as those taken by AI systems.

The following sections outline key areas that we recommend individuals to pay attention to while being active online. These recommendations would enable them to be aware of the data processing operations carried out and the ways to exercise their rights.

3.1. Key areas to pay attention to

3.1.1. Reviewing privacy policies, terms of service and default privacy settings

Agreeing to privacy policies allows controllers to process the personal data detailed in it. Individuals have the right not to consent to privacy policies without that action preventing them from accessing websites, services, etc., unless there is a legitimate reason (e.g.,

[8] Articles 2 and 3 of the GDPR.
[9] Article 4(7) GDPR: "*'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law*."

cookies necessary for the functioning of the website). Withdrawing consent should be as easy as providing it.

Reading and reviewing privacy policies and terms of service enables data subjects to understand how their personal data is collected, processed, and shared. This supports informed decision-making and facilitates the effective exercise of data protection rights.

It is recommended to examine default privacy settings – such as those related to chat history, search history, AI training, personalised advertising, analytics sharing, and automatic cloud backups. These settings are often enabled by default and can be adjusted according to individual preferences.

Additionally, for individuals using smart device at home, it is advisable to change default passwords and review how they process their personal data. Smart devices at home collect information related to the individuals' household activities, which may include sensitive or behavioural data. Understanding how such devices collect, process, and share information enables the identification and mitigation of potential risks, helping to minimise unnecessary or excessive data sharing within the home environment.

3.1.2. Exercising caution when sharing personal information

Before entering sensitive information – such as medical details, financial data, or personal images – into chatbots, applications, or online platforms, data subjects should exercise caution. Where feasible, the use of pseudonyms or the redaction of personally identifiable information (e.g., names, addresses, or age) can help protect an individual's identity.

Limiting the disclosure of personal information reduces the risk of misuse, profiling, or unauthorised access, thereby strengthening control over personal data.

Before interacting with AI systems, individuals are encouraged to consider the sensitivity of the information they provide. A useful guiding question might be: "If I were at a dinner with unfamiliar people, would I be comfortable sharing this information about myself or someone else?"

3.1.3. Keeping software and devices updated

Regularly updating software and firmware helps mitigate security risks, reducing the likelihood of data breaches or unauthorised access to personal data.

3.1.4. Managing application and device permissions

It is advisable to regularly review applications that have access to a device's microphone, camera, location data, contacts, and files. Where certain permissions are not essential, the data subject may choose to disable or enable only when necessary – e.g., restricting access to photos or selectively sharing them with specific applications. Adjusting permissions in this way limits unnecessary access to personal data, ensuring that only essential information is processed.

3.2. Data subject rights

If individuals follow the recommendations set out in the previous section, they should already start to grasp the type of personal data controllers have and use. In addition, the GDPR grants rights to individuals which can be exercised by contacting said controllers. If

the exercise of such rights is requested, controllers must answer within a month. This period may be extended by up to two additional months, if justified.

3.2.1. Right to information

Articles 13 and 14 of the GDPR provide for a right to information which imposes a duty on controllers to inform individuals on the processing activities carried out. This information should enable individuals to take informed decisions and exercise their data protection rights. This information must be presented in clear and accessible language and is generally found in the privacy policy.

The GDPR distinguishes situations where personal data is collected directly (consent forms, website subscriptions, etc.) from the data subject and those where it is collected indirectly (web scraping, licensing agreements, etc.). When personal data is collected indirectly, art. 14 of the GDPR demands controllers to inform the data subject within a month after the collection.

Controllers must communicate the following information: identity and contact details of the controller; purpose(s) and legal base(s) for the processing operation; data retention periods; the rights of data subject; details on data transfers; and information related to automated decision-making. Under Article 14 of the GDPR, controllers are also required to disclose the data sources and categories of personal data collected.

3.2.2. Right of access

Under Article 15 of the GDPR, data subjects have the right to obtain confirmation as to whether their personal data is being processed. When exercised, controllers must provide access to details such as the purpose and categories of data processed; data recipients, if any; storage period; data protection rights; the right to lodge a complaint with a supervisory authority; the source of the data when not obtained directly from the individual; and any automated decision-making, including profiling, with meaningful information about the logic involved, the significance and the envisaged consequences of such processing for the data subject.

Additionally, data subjects have the right to obtain a copy of the personal data undergoing processing, free of charge, if that copy is necessary to understand the context in which the data processing activity is carried out.[10]

3.2.3. Right to erasure

Under Article 17 of the GDPR, data subjects can request the erasure of their personal data without undue delay when certain conditions apply:

- when the personal data is no longer necessary for the original purpose;
- when the data subject withdraws its consent, and there is no other legal ground for the processing;

[10] According to the CJEU, in C-487/21 (*Österreichische Datenschutzbehörde* and CRIF), a "copy" may include parts of original documents or entire documents, if necessary to ensure the effectiveness of the right of access, while also respecting the rights and freedoms of others. The format must allow the data subject to retain and review the data, and in some cases (e.g., handwritten notes or voice recordings), the format itself may be integral to the personal data.

- when the data subject objects to processing under Article 21(1) of the GDPR and there are no overriding legitimate grounds;
- when the personal data has been unlawfully processed;
- when the personal data must be erased to comply with a legal obligation; or
- when the personal data have been collected in relation to the offer of information society services.

In situations where the controller communicated the personal data to third party recipients or made it public, it has to take appropriate measures to ensure the erasure of these personal data[11].

3.2.4. Right to object

Article 21 of the GDPR grants data subjects the right to object to the processing of their personal data. Once an objection is made, the controller must stop the processing unless it can demonstrate overriding legitimate grounds.

In the case of processing for direct marketing purposes, the right to object is absolute and does not require justification.

On a side note, both the Belgian and French data protection authorities have published guidance outlining steps that individuals can take to prevent tech companies (e.g., Meta, TikTok, Microsoft, X) from using their personal data to train their AI systems. These steps are available here and here.

3.2.5. Right to restriction of processing[11]

Under Article 18 of the GDPR, data subjects have the right to request the restriction (limitation) of data processing activities when:

- the accuracy of the personal data is disputed by the data subject;
- the data has been processed unlawfully;
- the controller no longer needs the data for its original purpose, but the data subject still requires them for the establishment, exercise, or defence of legal claims;
- the data subject has objected to the processing (Article 21 of the GDPR), while the balancing exercise between controller's interest and the data subject's is being carried out.

During such a restriction, personal data may only be processed (excluding storage) with the data subject's consent or for legal claims or for the protection of the rights of others (natural or legal person) or for reasons of important public interest of the Union or of a Member State. The data subject must be informed before the restriction is lifted.

The right to restriction of processing differs from right to object, as it results in a pause on all processing operations, rather than just specific purposes.

[11] Article 19 GDPR: "*The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.*"

3.2.6. *Right to rectification*[11]

Article 16 of the GDPR provides data subjects with the right to request the correction of inaccurate personal data and the completion of incomplete data (including by providing supplementary statements).

If the data has been disclosed to third parties, the controller must inform them of the rectification, unless this proves impossible or involves disproportionate effort.

3.2.7. *Right to data portability*

Under Article 20 of the GDPR, data subjects have the right to receive their personal data in a structured, commonly used, machine-readable format. They also have the right to transmit it to another controller when the processing is: based on the data subject's consent; necessary for the performance of a contract; or carried out by automated means. Where technically feasible, data must be directly transmitted to the new controller.

3.2.8. *Right not to be subject to automated decision-making*

Article 22 of the GDPR grants data subjects the right not to be subject to decisions based solely on automated processing, including profiling, which produce legal effects concerning them or similarly significantly affect them[12].

A processing operation is not solely automated when there is a meaningful human involvement. This entails the implication of an individual with sufficient authority to alter the outcome of the processing activity. [xii]

Automated decision making is allowed when it is necessary for the performance of a contract, with the explicit consent of the data subject or if it is authorized by law. In such cases, controllers must ensure that data subjects have the right: to obtain human intervention[13] on the part of the controller; to express their point of view; and, to contest the decision.

In addition, under Article 15(1)(h) of the GDPR, data subjects are granted a right to an explanation as to the functioning of the mechanism involved in automated decision making[14,15]. This entails the clear communication of the procedures and principles applied to understand how personal data have been used in the automated decision making[16].

---

[12] According to the WP29 Guidelines on Automated individual decision-making and Profiling (2018), decisions may be considered to have similarly significant effects if they have the potential to: significantly affect the circumstances, behaviour or choices of the individuals concerned; have a prolonged or permanent impact on the data subject; or lead to the exclusion or discrimination of individuals.

[13] When it comes to High-Risk AI systems (Chapter III of the AI Act), deployers shall assign human oversight to natural persons who have the necessary competence, training and authority, as well as the necessary support (Article 26(2) of the AI Act). Article 14 of the AI Act set the requirements and goals of human oversighting in High-risk AI systems.

[14] *Dun & Bradstreet*, §57.

[15] Furthermore, as a general rule, Article 86 of the AI Act states that individuals have the right to receive a clear explanation of the role the High-Risk AI system played in the decision-making process if the decision significantly affects their health, safety, or fundamental rights.

[16] *Dun & Bradstreet*, §61.

3.3. Exercising data subject rights

When a controller is believed to be misusing personal data, or when it becomes necessary to verify what data is being processed, data subjects can exercise their data protection rights.

3.3.1. Engaging directly with the controller

Data subjects can exercise their rights by reaching out to the controller.

- Use of a template letter: The Belgian DPA developed tailored template letters **here**. They provide standardised formats to assist in formulating such requests. The letter should clearly outline the nature of the request and the legal basis on which it is made.
- Identification of the controller's contact details: Where available, the request should be addressed to the designated Data Protection Officer (DPO), whose contact information is provided in the privacy policy. If no DPO is specified, the request may be sent to the controller's general contact address.
- Retention of evidence: A copy of the request should always be retained by the data subject. This serves as evidence in the event that further steps, including regulatory intervention, becomes necessary.
- Allowing time for response: Under data protection law, controllers are required to respond within one month of receipt of the request. In exceptional cases, this period may be extended by up to two additional months, with a justification provided.

3.3.2. Involving the Belgian DPA

If the controller fails to respond, or if the response is considered inadequate, the data subject may escalate the matter to the relevant supervisory authority (**contact form link**):

- Requesting mediation (**contact form link**): Mediation is often the most efficient method to solve disputes. The Belgian DPA may request that the controller addresses the data subject's rights appropriately.
- Filing a formal complaint (**contact form link**): Where mediation does not result in resolution, a formal complaint may be lodged with the Belgian DPA. This may lead to enforcement measures, including but not limited to a warning, an administrative fine, or an immediate order to cease specific processing activities.

References:

- Andreas Krause, Jonas Hübotter. Probabilistic Artificial Intelligence (2025). Available at: https://arxiv.org/pdf/2502.05244
- Bart Custers, Helena Vrabec. Tell me something new: data subject rights applied to inferred data and profiles, Computer Law & Security Review, Volume 52, 2024, 105956, ISSN 2212-473X, https://doi.org/10.1016/j.clsr.2024.105956. (https://www.sciencedirect.com/science/Article/pii/S0267364924000232)
- Bygrave, in Kuner, Bygrave, Docksey. The EU General Data Protection Regulation (GDPR): A Commentary, Article 22 GDPR, p. 533 (Oxford University Press 2020)
- Daniel J. Solove. Artificial Intelligence and Privacy, 77 Fla. L. Rev. 1 (2025). Available at: https://scholarship.law.ufl.edu/flr/vol77/iss1/1
- Enrico Glerean. Fundamentals of Secure AI Systems with Personal Data (2024). EDPB.
- European Commission. Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 20241689 (AI Act), at https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-ai-system-definition-facilitate-first-ai-acts-rules-application
- European Data Protection Board. Respect Individuals' Rights (SME Guide). Available at: https://www.edpb.europa.eu/sme-data-protection-guide/respect-individuals-rights_en
- European Data Protection Supervisor. Guidelines on the protection of personal data processed by mobile applications provided by European Union institutions (2016). Available at: https://www.edps.europa.eu/sites/default/files/publication/16-11-07_guidelines_mobile_apps_en.pdf
- European Data Protection Supervisor. Guidelines on the Rights of Individuals with regard to the Processing of Personal Data (2014). Available at: https://www.edps.europa.eu/sites/default/files/publication/14-02-25_gl_ds_rights_en.pdf
- European Data Protection Supervisor. Tech Dispatch #2/2023 - Explainable Artificial Intelligence (XAI). Available at: https://www.edps.europa.eu/system/files/2023-11/23-11-16_techdispatch_xai_en.pdf
- Marco Almada. Law & Compliance in AI Security & Data Protection (2024). EDPB.
- OECD (2024). "Explanatory memorandum on the updated OECD definition of an AI system", OECD Artificial Intelligence Papers, No. 8, OECD Publishing, Paris, at https://doi.org/10.1787/623da898-en
- 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
- Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828

- WP29, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679', 17/EN WP251 rev.01, 6 February 2018.

---

[i] *Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 20241689* (AI Act), p. 2.
[ii] More information on: Recital 12 AI Act.
[iii] *Guidelines on the definition of an artificial intelligence system established by Regulation* (EU) 20241689 (AI Act), p. 5.
[iv] Recital 12 AI Act.
[v] Marco Almada - *Law & Compliance in AI Security & Data Protection*, p. 22-24.
[vi] Enrico Glerean - *Fundamentals of Secure AI Systems with Personal Data*, p. 40-44.
[vii] Daniel J. Solove, *Artificial Intelligence and Privacy*, 77 Fla. L. Rev. 1 (2025). Available at: https://scholarship.law.ufl.edu/flr/vol77/iss1/1 p. 59-62.
[viii] Daniel J. Solove, *Artificial Intelligence and Privacy*, p. 6, 55-66.
[ix] Daniel J. Solove, *Artificial Intelligence and Privacy*, p. 16-18, 36-37, 39-40.
[x] Andreas Krause, Jonas Hübotter (2025) - *Probabilistic Artificial Intelligence*. Available at: https://arxiv.org/pdf/2502.05244 p.1-2, 37-38.
[xi] Marco Almada - *Law & Compliance in AI Security & Data Protection*, p. 25-26.
[xii] WP29, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, 17/EN WP251 rev.01, 6 February 2018, p. 21.
Bygrave, in Kuner, Bygrave, Docksey, *The EU General Data Protection Regulation (GDPR): A Commentary*, Article 22 GDPR, (Oxford University Press 2020) p. 533.