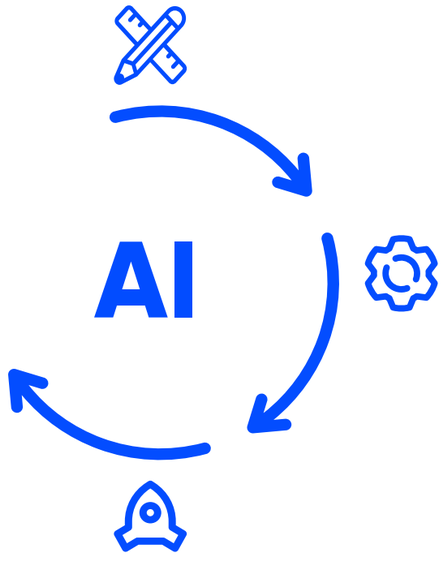
HOW IS THE AI LIFECYCLE REGULATED?

Several regulatory regimes apply to developers during the lifecycle of an AI system. In this brAInfood, we highlight various regulatory regimes which should be taken into account at different stages of the lifecycle of an AI system. We only highlight the regimes that we consider to be highly relevant, so this is not an exhaustive list.

Knowledge Centre Data & Society (January 2024). How is the AI lifecycle regulated? Brussels: Knowledge Centre Data & Society.



	DESIGN	DEVELOP	DEPLOY
	The design phase includes the definition of the problem which the AI system will address. It also includes the collection and preparation of data, and the division of data into training, validation, and testing sets.	In this phase the AI system is created. It is trained with data, making it better through repeated adjustments. It is further tested and refined to ensure that its outcomes are accurate and fit for purpose.	Once it is sufficiently tested and fulfils its operational requirements, the AI-system can be deployed in a real environment.
CONTRACT LAW	Training data, existing models, and other tools such as computing power may be subject to licences and other contract terms. Developers should review the contract terms and follow them if they agree to using these tools.	Contracts should be put in place governing the development, ownership, use, and sharing of the AI system and its outputs. Clear ownership rights must be established for the AI algorithms/software, data sets and other intellectual property assets developed during this phase, including developments by (sub)contractors and employees. Other contractual safeguards (such as confidentiality) may also be desirable.	Terms and conditions (B2C and/or B2B) need to be presented to users before they interact with the AI system, outlining the permissions, restrictions, and expectations for using the system.
AI ACT	Adopts a risk-based approach classifying AI systems into four categories based on potential risk: unacceptable, high, limited, and minimal risk. Data used in the development of high-risk AI systems must comply with certain quality criteria set out in the AI Act (e.g. relevance, completeness, etc.).	Developers of high-risk AI systems must comply with requirements on risk management, technical documentation, transparency, record keeping, human oversight, etc. Certain high-risk AI systems may also need to be subject to a Fundamental Rights Impact Assessment before deployment.	Several high-risk AI systems must undergo conformity assessment procedures (internal or third-party) prior to entering the market or first use. Some categories of high-risk AI systems will also need to be registered in a dedicated EU database. Certain AI systems must also comply with transparency obligations. Providers must take corrective actions if their high-risk AI systems on the market is not in conformity with the AI act and should be aware of possible complaints from persons affected by the AI system.
DATA PROTECTION	The **GDPR** applies to the collection, use and other processing of personal data. If personal data is needed for the training of an AI-system, developers should comply with GDPR requirements. These obligations are broad and include for example data minimisation, a lawful basis for processing and purpose limitation when using the data (with exceptions for public interest and statistical purposes).	A **Data Protection Impact Assessment (DPIA)** can assist in identifying data protection risks and related solutions. In that way, necessary safeguards can be built into the AI-system. **By design:** Data-protection principles should be implemented in the design of the AI-system through technical means (where possible). This includes, for example, integrating data minimisation in the system (by using anonymous or pseudonymous data) or storage limitation (by automatically removing data which is no longer required). **By default:** The AI-system should be designed in a way that when it is used, it by default uses the most data protection friendly settings (e.g. collect only the personal data strictly required for the primary purpose of the system, but allow users to provide more data for secondary functionalities).	**GDPR:** Personal data processing in a deployed AI system should be based on a lawful ground and be done in a fair and transparent manner. The deployer must enable the data subject's rights. If relevant, applicable restrictions regarding automated decision-making also need to be taken into account.
OTHER	**Copyright:** If the dataset used to train the AI system contains literary or artistic works, these are protected by copyright. Their reproduction requires permission from the copyright holder unless text-and-data mining exceptions are applicable. **Data Act:** Contains rights on fair access to and use of data. This includes access mechanisms for data generated by connected devices, and rules for unfair contract terms related to data access and use. Developers should be aware of these possible data access mechanisms and of contract terms that they should not accept. **Deontological or professional secrecy obligations:** If training data originates from or is used in the context of a regulated occupation, specific obligations may apply restricting the possible (re-)use of data.	**Technical norms and standards:** Crucial for ensuring quality, and security of the AI system. Certain harmonised (EU-) standards also provide the developer with presumptions of conformity (for example the Regulation on General Product Safety and schemes under Cybersecurity Act) or allow them to use internal conformity assessments (for example the AI Act). **Patent law:** Apart from hardware, new software, data structures or formats may be protected under patent law if they have a technical effect and fulfil the other patentability requirements. Developers should be aware that the use of patented technologies requires permission.	**Consumer protection:** In situations involving consumers, information obligations, rules on unfair commercial practices and requirements for consent need to be considered by the AI-provider, including when AI is the subject of the agreement or is used to conclude the contract. **Copyright:** Developers must put in place appropriate disclaimers or warranties for the output of the AI system. Particularly, they should define their position on outputs that may infringe on a third-party's copyright. **Digital Service Act:** The use of automated tools (including AI systems) for content moderation by intermediary service providers, hosting providers and online platforms is subject to reporting and transparency obligations. **Liability** • Contractual liability: Developers may be contractually liable if the system fails to perform or is otherwise non-conform to what was agreed on. • Non-contractual liability: Use of an AI-system may give rise to non-contractual liability. The AI Liability Directive proposal lays down rules for the disclosure of evidence and presumptions to the benefit of a person claiming damages caused by the involvement of an AI system. • Product liability: producers are liable for damage caused by their products, regardless of whether they were negligent or not (EU Product Liability Directive).

Knowledge Centre Data & Society

Artificial Intelligence Flanders