Development of AI Systems: What should be checked?

The CNIL provides **a checklist of points to verify, based on its recommendations for the development of AI systems compliant with the GDPR.**

This checklist is intended for designers and developers of AI systems (product managers, developers, data protection officers, legal teams, chief information security officers, etc.) in order to secure all stages of the development of an AI system, from data collection to integration, including model training and annotation. This checklist aims to ensure that, from the very start, the principles of the GDPR are correctly implemented: purpose limitation, data minimization, security, information, data subject rights, transparency, and governance.

Please note: Where applicable, the obligations established by the EU AI Act should also be considered during the development of these systems. These obligations are not addressed in this checklist.

SHEETS			MEASURES	
1	Determine the applicable legal framework and your responsibility	Identify whether the GDPR applies	Identify whether the training dataset contains **personal data** (including data obtained through web scraping).	☐
			Analyze whether the GDPR applies to the model learned from training dataset containing personal data or whether it can be presumed to be anonymous. • To do this, establish the necessity of conducting re-identification attacks on the AI model, the depth of these attacks, and the likelihood of extraction of personal data, providing as much detail as possible by data type.	☐
			If you believe that a system incorporating a non-anonymous AI model may fall outside the scope of the GDPR, ensure that the measures put in place are sufficiently effective and robust to render the likelihood of re-identification of individuals insignificant. • This assessment necessarily involves conducting re-identification attacks on the AI system.	☐
			Implement a process for regularly reassessing the anonymity of the model or system.	☐
		Define the responsibilities of the relevant actors	Determine your **responsibility** and that of other parties involved in the processing of personal data (data controller, joint controller, or processor).	☐
			Where applicable, make sure you sign a contract to **outline joint liability.**	☐
			Where applicable, make sure you enter into a contract to **document the instructions** given to your subcontractors.	☐
2	Define the purposes and choose the legal basis	Define the purposes	Clarify the **purpose(s)** of the project from the design phase • If it is general-purpose AI, refer to the type of system developed (e.g., the development of a large language model, a computer vision system) as well as the technically feasible features and capabilities.	☐
		Identify the legal basis	Identify the **legal basis** for each processing (consent, legitimate interest, etc.).	☐
			Where applicable, document the **methods used to obtain consent** and retain proof thereof (Article 6.1.a of the GDPR).	☐
			Where applicable, ensure that you have a **valid contract** and that the processing is necessary to fulfill the purpose of the contract (Article 6.1.b of the GDPR).	☐
3	Where applicable, assess the validity of the legal basis for legitimate interest (Article 6.1.f of the GDPR)	Verify the existence of a legitimate interest	Define clearly **the objective pursued.**	☐
			Verify that **the interest does not conflict with other regulatory obligations** (Digital Services Act, Artificial Intelligence Act, etc.).	☐
		Assess the need for processing	Ensure that the processing of personal data is **necessary to achieve the defined purpose.**	☐
			Check that **less intrusive methods** (e.g., anonymization, synthetic data) cannot achieve the same results.	☐
			Ensure that the algorithmic techniques used for data processing (e.g., deep convolutional neural networks, support vector machines, etc.) **consume as little personal data as possible** for the intended purpose. If necessary, document the need to use machine learning, particularly deep learning.	☐
			Check whether design choices can be taken into account with a view to data protection by design (federated learning, secure multi-party computation, homomorphic encryption, etc.).	☐
		Balancing the interests at stake	Ensure and document that the data subjects can **reasonably expect** this processing.	☐
			Where applicable, implement and document **appropriate and sufficient safeguards to limit the impact of processing on data subjects** (e.g., provide for the rapid anonymization of collected data or, failing that, pseudonymize the data collected, adopt measures to limit the risks of memorization, extraction, regurgitation in the context of generative AI or attacks on AI models or systems, provide for a discretionary and prior right to object, etc.).	☐
			Where applicable, implement **appropriate safeguards for web scraping** (e.g., limit collection to freely accessible data, establish a list of sites from which collection would be excluded by default because they contain particularly intrusive data).	☐

SHEETS			MEASURES	
4	In case of data reuse, perform additional tests and checks	If you reuse your own data	If the training purpose of your model was not defined at the time of data collection, ensure that its compatibility with the original purpose through a **compatibility test** (unless you are authorized by the data subjects' consent or by law, or if you reuse the data for statistical or scientific research purposes): • Is there a link between the initial purpose and the new AI purpose? • Does the context of the initial collection reasonably allow for this reuse? • What is the type and nature of the data (identifiers, sensitive data, etc.)? • What are the possible consequences for individuals? • What technical and organizational safeguards are in place (pseudonymization, etc.)?	□
		If you reuse publicly available data or data acquired from a third party (e.g., data broker)	Check that you are not reusing a dataset that was **clearly created illegally:** • Is the source of the data clearly identified and documented? • Is the dataset the result of a crime or offense (leakage, theft, etc.) or has it been the object of a conviction or public sanction by a competent authority that has resulted in its removal or prohibition from use? • Are the conditions under which the data was collected sufficiently documented? • Does the dataset contain any sensitive or infringing data, or are enhanced checks carried out to ensure that the processing is lawful if so?	□
5	Limit the data processed to what is relevant and necessary (data minimization)	Selection of strictly necessary data	Identify the data that is essential to achieving your objectives and favor less intrusive formats (e.g., age range rather than full date of birth).	□
			Regarding data volume, justify the number of data subjects, historical depth, and granularity.	□
			Justify the need to **process highly personal data.**	□
			Regarding data types, evaluate the use of real data and synthetic, pseudonymized, or anonymized data.	□
			Identify data sources.	□
		Implement specific measures in the event of web scraping	Define **specific collection criteria** in advance.	□
			Exclude the collection of **certain categories of data** when they are not necessary, using filters where possible or, failing that, by excluding certain types of sites that structurally contain these categories of data.	□
			Exclude from data collection any **websites that explicitly oppose the scraping** of their content, for example through the use of robots.txt files or the implementation of CAPTCHA.	□
		Specific precautions for sensitive data	Justify the **need** to process sensitive data.	□
			Identify **exceptions to the principle prohibiting the processing of sensitive data** (Article 9.2 of the GDPR).	□
			Provide for **enhanced security measures** (pseudonymization, etc.).	□
			Immediately delete, if possible automatically, any sensitive data collected incidentally and residually during web scraping.	□
		Organization of data collection and preparation	**Clean up** the data (inconsistencies, duplicates, etc.).	□
			Identify the **data that is truly relevant** to the task and delete data that is not relevant for learning.	□
			Apply **data protection techniques from the design stage (**e.g., generalization, randomization, pseudonymization, anonymization, etc.).	□
		Justification and validation of design choices	Conduct a **test run** with fictitious, synthetic, or anonymized data.	□
			Consult **an ethics advisor or committee** on issues related to ethics and the protection of individuals' rights and freedoms.	□
		Continuous reassessment	Establish a process for regularly reviewing the relevance of the data collected.	□
			Establish mechanisms for deleting unnecessary or obsolete data.	□
6	Define and monitor data retention periods	Define a clear retention policy from the design stage	Define a specific retention period for each phase of the AI project lifecycle (development, maintenance, improvement, etc.).	□
		Retention during the development phase	Ensure that data is only accessible to authorized persons during development.	□
			Establish a process for archiving or deleting data at the end of the development phase, unless it is necessary to retain the data for maintenance or improvement of the product.	□
		Retention for the purpose of maintaining or improving the product	Document the need to retain data beyond development, particularly for product maintenance or improvement.	□
			Verify that data is stored on a secure, segmented medium.	□
			Verify that access is strictly limited to individuals responsible for product maintenance or improvement.	□
			Implement an automatic deletion plan once the improvement has been made.	□

SHEETS			MEASURES	
7	Ensure transparency of the processing		**Inform** data subjects in a clear and easily accessible manner of all the information provided for in Articles 13 and 14 of the GDPR.	□
			When data is not collected directly from individuals, document, where applicable, the fact that individual information would **require disproportionate effort** (Article 14.5.b of the GDPR) and make the information publicly available (website, etc.).	□
			If web scraping involves a limited number of sites, **provide precise information** on the sources used. If there are a large number of sources, **provide the categories of source sites**, at least those that pose the greatest risk to individuals.	□
			When the model itself is subject to the GDPR, **inform individuals about the data stored** and provide all the information required by Articles 13 and 14 of the GDPR.	□
8	Respect the rights of individuals	Implementation of procedures for rights management	Inform individuals of **the risk of data regurgitation** in the case of generative AI, the **measures taken to limit these risks, and the existing recourse mechanisms** (e.g., the possibility of reporting an instance of regurgitation).	□
			Establish a **procedure for notifying recipients, in particular users, of any request** for rectification, erasure, or restriction of data, unless such communication proves impossible or requires disproportionate effort.	□
		Manage identification of individuals	For generative AI, **set up an internal process** (like using a list of selected queries) to see what data the model might have stored about the person based on the input.	□
			If it is not possible to identify a data subject within the model but they are identified in a training dataset, inform them of the risk of model memorization.	□
			If it is **not possible to identify a data subject** in the training dataset or within the model, inform them.	□
			Inform the data subject of **any additional information** that can be provided to help identify them (e.g., pseudonym, sample of their data).	□
			Establish a process **for deleting this additional data** after the request has been processed.	□
		Selecting a technical solution to ensure compliance with model rights	In principle, **plan for a model retraining** process. • Retraining can be periodic to limit costs and fulfill multiple requests for rights exercises at the same time	□
			Provide users with **an updated version of the model**, possibly by contractually requiring them to use only a regularly updated version	□
			Where applicable, document the fact that **retraining the model is disproportionate** (temporarily or permanently).	□
			If retraining is disproportionate, **implement filters or other robust measures** on the outputs of the AI system.	□
			Where applicable, **general rules preventing the generation of personal data should be preferred** to a simple "blacklist" of individuals who have exercised their rights.	□
9	Ensure data annotation compliance		Ensure that annotations include only the information required to fulfill the purpose and that they remain objective.	□
			Conduct **regular reviews** to ensure that labels remain relevant.	□
			Establish a **continuous verification procedure** to monitor the quality of annotation: define an annotation protocol, applying the principles of accuracy and minimization, and involve an ethics advisor or committee (good practice).	□
			Inform data subjects about the data annotation phase.	□
			Ensure that **internal rights management procedures and terms and conditions for exercising rights** include annotation (right of access, rectification, erasure, restriction, portability, and objection)	□
			Where applicable, verify that sensitive data is processed in accordance with an exception to the data prohibition principle (Article 9.2 of the GDPR).	□
			Implement **specific measures** to address the increased risk to data subjects: annotate according to objective and factual criteria, limit annotation to the context of the data, strengthen the annotation verification stage, increase the security of annotated data (e.g. by performing annotation processing internally, processing data locally, and ensuring its security through encryption, logging, and stronger access restrictions) and consider the risk of regurgitation and inference of sensitive data on models trained from them.	□
			Train the individuals responsible for annotation on the principles relating to data protection.	□

SHEETS			MEASURES	
10	Ensure data security		Ensure that the security measures applied to the training data are adequate and fit for purpose (see the practice guide for the security of personal data).	□
			Ensure that the security measures applied to system development are adequate and appropriate, notably by using verified development tools, libraries, and, where applicable, pre-trained models.	□
			Ensure that the measures in place to govern the system's operation are adequate and appropriate for example, by using verified import and storage formats such as safetensors, monitoring AI outputs with filters, and implementing watermarking techniques.	□
			Manage data access permissions, keep records of all access, and regularly review those logs.	□
			Implement and monitor an action plan to ensure that safety requirements are met.	□
11	Analyze risks and conduct a data protection impact assessment (DPIA)		Carry out a DPIA if the model training processing presents high risks according to the criteria established by the European Data Protection Board (innovative use, large scale, sensitive data, vulnerable individuals, etc.).	□
			Include **specific AI risks** (automated discrimination caused by bias introduced during development, risk of producing fictitious content about a real data subject, risks related to known attacks specific to AI systems, etc.) and take **appropriate measures.**	□