CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

PROTÉGER les données personnelles
ACCOMPAGNER l'innovation
PRÉSERVER les libertés individuelles

CNIL's first recommendations for GDPR-compliant AI systems

EDPS - DPOs 54th meeting
19 June 2024

Erevan Malroux
AI Department

CNIL.

Summary

- **Introduction**

- The context of the AI how-to sheets
- The content of CNIL's recommendations
- Recent and future work

CNIL'S MISSIONS

Informing people and protecting their rights

Guide compliance and provide advice

Control and sanctions

Anticipate and innovate

Artificial intelligence department

CNIL's AI Department

- 5 people with diverse backgrounds:
  - 2 Ph. D. in ML,
  - 1 Ph.D. in cognitive science,
  - 1 AI Engineer,
  - **1 Privacy Legal Expert.**

- Missions:
  - Apprehend: Technology and Scientific Watch, Improve AI's CNIL Culture
  - **Guide: Enable and guide the development of privacy-friendly AI**
  - Federate: Partner with institutions, researchers, and the AI ecosystem
  - Audit: Develop audit and investigations methodologies

Summary

- ✓ Introduction

- ❑ **The context of the AI how-to sheets**

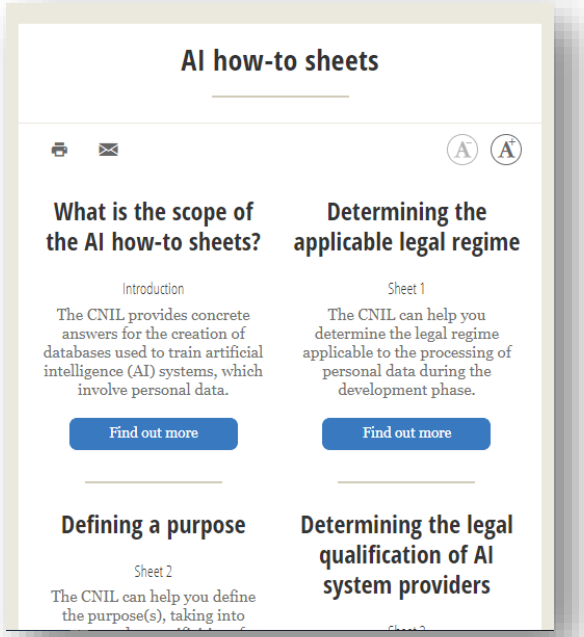
- ❑ The content of CNIL's recommendations
- ❑ Recent and future work

CNIL's how-to sheets on AI systems

- Why?
  - Acceleration of AI development
  - Specificities of the AI context

- How?
  - Illustrated guidance based on prior concertations
  - Open to public consultation

- What does it cover?
  - Key GDPR principles applied
    - Purpose
    - Controllership
    - Legal basis
    - Minimisation, etc.



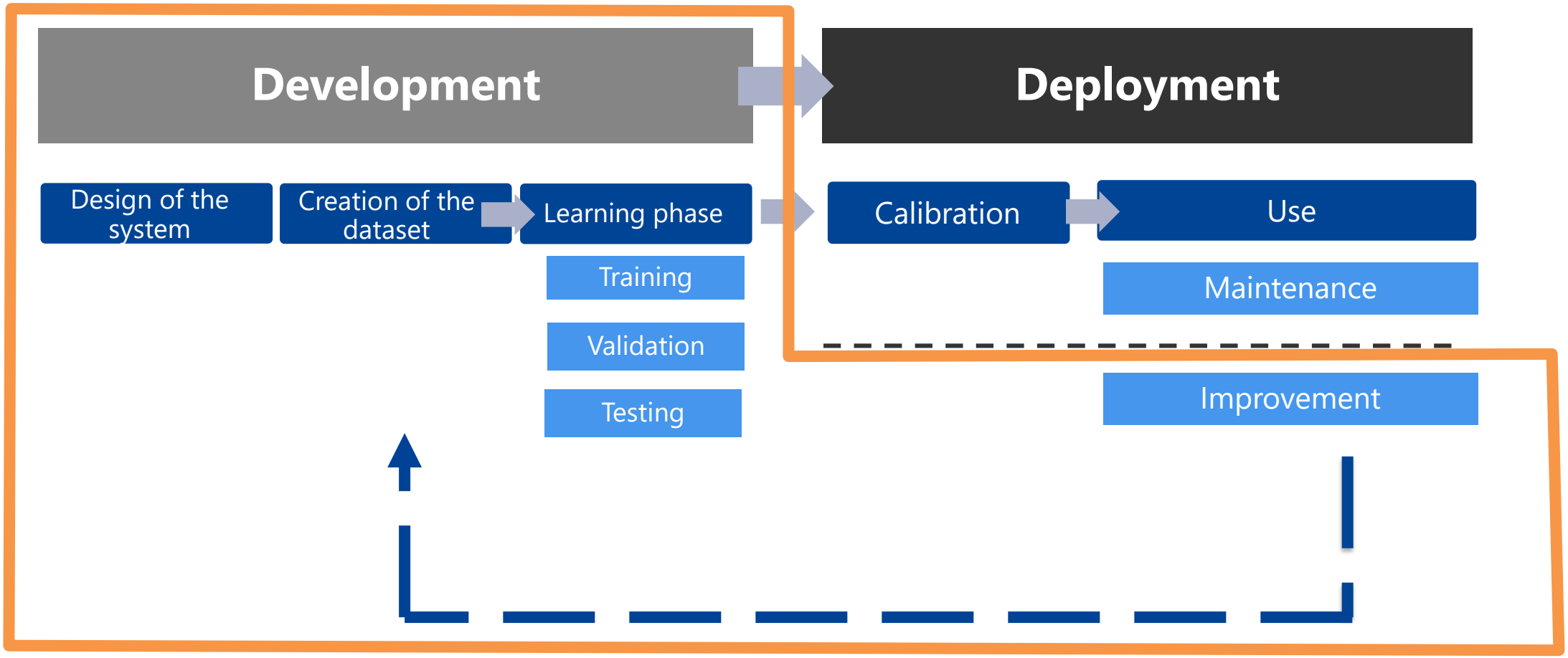
EN available

Definition of AI systems

- These recommendations concern the development of systems based on AI techniques and involving **the processing of personal data.**

- In practice, the AI systems concerned include **systems based on machine learning** (supervised, unsupervised, reinforcement) and those based on **logic and knowledge** (knowledge bases, inference and deduction engines, symbolic reasoning, expert systems, etc.), as well as hybrid approaches.

Scope of the first how-to sheets



CNIL.

Summary

- ✓ Introduction
- ✓ The context of the AI how-to sheets

- ❑ **The content of CNIL's recommendations**

- ❑ Recent and future work

Differences between the two phases

Sheet 2 - Defining a purpose

The operational use of the AI system is precisely identified from the development phase

If the purpose in the deployment phase is determined, explicit and legitimate, the purpose in the development phase is also considered as such.

The operational use of the AI system is not clearly defined already in the development phase (general purpose AI systems)

The purpose of the processing must refer cumulatively to:

- the "type" of system developed
- Technically feasible functionalities and capabilities

It is recommended that the purpose also includes:

- the most at-risk foreseeable capacities
- features excluded by design
- as far as possible, the conditions of use of the AI system

The AI system is developed for scientific research purposes

It may be accepted that the degree of precision of the purpose is lower or that the purposes of the research are not specified in their entirety, given the difficulties in fully identifying it from the start of the work.

Sheet 2 - Defining a purpose

The operational use of the AI system is precisely identified from the development phase	**The operational use of the AI system is not clearly defined already in the development phase (general purpose AI systems)**	The AI system is developed for scientific research purposes
If the purpose in the deployment phase is determined, explicit and legitimate, the purpose in the development phase is also considered as such.	The purpose of the processing must refer cumulatively to: • the "type" of system developed • Technically feasible functionalities and capabilities	It may be accepted that the degree of precision of the purpose is lower or that the purposes of the research are not specified in their entirety, given the difficulties in fully identifying it from the start of the work.

For example:

☹ Development of AI models (no type or technical capabilites)

☹ Development of a generative AI model (no potential capabilities)

☺ Development of a large language model (LLM) capable of answering questions, generating text according to context (emails, reports, etc.), translating, summarising and correcting text, classifying text, analysing feelings, etc.

Sheet 2 - Defining a purpose

The operational use of the AI system is precisely identified from the development phase

If the purpose in the deployment phase is determined, explicit and legitimate, the purpose in the development phase is also considered as such.

The operational use of the AI system is not clearly defined already in the development phase (general purpose AI systems)

The purpose of the processing must refer cumulatively to:

- the "type" of system developed
- Technically feasible functionalities and capabilities

It is recommended that the purpose also includes:

- the most at-risk foreseeable capacities
- features excluded by design
- as far as possible, the conditions of use of the AI system

The AI system is developed for scientific research purposes

It may be accepted that the degree of precision of the purpose is lower or that the purposes of the research are not specified in their entirety, given the difficulties in fully identifying it from the start of the work.

Sheet 2 - Defining a purpose

The operational use of the AI system is precisely identified from the development phase	The operational use of the AI system is not clearly defined already in the development phase (general purpose AI systems)	The AI system is developed for scientific research purposes
If the purpose in the deployment phase is determined, explicit and legitimate, the purpose in the development phase is also considered as such.	The purpose of the processing must refer cumulatively to: • the "type" of system developed • Technically feasible functionalities and capabilities	It may be accepted that the degree of precision of the purpose is lower or that the purposes of the research are not specified in their entirety, given the difficulties in fully identifying it from the start of the work.

- The concept of "scientific research" has a **broad scope** in the GDPR. The CNIL has **specified the criteria for defining scientific research,** which concerns many research and development activities, including in the private sector.
- The status of scientific research **simplifies certain obligations.**

Sheet 2 - Defining a purpose

The operational use of the AI system is precisely identified from the development phase	The operational use of the AI system is not clearly defined already in the development phase (general purpose AI systems)	The AI system is developed for scientific research purposes
If the purpose in the deployment phase is determined, explicit and legitimate, the purpose in the development phase is also considered as such.	The purpose of the processing must refer cumulatively to: • the "type" of system developed • Technically feasible functionalities and capabilities	It may be accepted that the degree of precision of the purpose is lower or that the purposes of the research are not specified in their entirety, given the difficulties in fully identifying it from the start of the work.

For example:

The development of an AI system for a proof of concept to demonstrate the robustness of machine learning requiring less training data, in a documented scientific approach intended for publication.

Sheet 3 – Determining responsibility

The provider of the AI system

Controller

The natural or legal person who determines the purposes and means of the processing

For example:
If the provider is at the initiative of the development and builds the learning database for its own account.

If the provider uses a service provider to collect and process the data according to his instructions, the latter will be the provider's processor.

Sheet 3 – Determining responsibility

The provider of the AI system

Joint controller

For example:
If the provider builds the learning database with other controllers for a purpose defined together.

Sheet 3 – Determining responsibility

The provider of the AI system

Processor

The natural or legal person who processes data on behalf of the controller

For example:
If the provider develops an AI system on behalf of one of its customers, which determines the purpose, means and techniques to be used.

On the other hand: if the customer gives only one objective to be achieved but the provider designs the AI system, the provider is responsible for the processing.

Creating a training dataset

The controller itself collects the data for the purpose of creating a training dataset

- Directly from individuals
- Indirectly (e.g. on the Internet)

The controller reuses data previously collected for another purpose

Data originally collected by the controller itself for another purpose	A publicly accessible dataset	A dataset acquired from a third party
		
Carry a "compatibility test" on the new purpose	Verify the absence of manifest unlawfulness of the dataset	Inquire about the lawfulness of the initial processing (e.g. thanks to the conclusion of an agreement)

Ensure that the dataset is in compliant with the applicable regulations

Training dataset

Sheet 4 – Defining a legal basis

Consent	Legitimate interest	The public interest mission	Other legal bases
• **Freey given** • **Specific** • **Informed** • **Unambiguous**	• **Legitimacy of** the interest • **Necessity** of data processing • **No disproportionate interference with** the interests and rights f the individuals	• **Mission of public interest provided for in a text** • **Necessity** of the processing to specifically carry out this task, in a relevant and appropriate manner	The legal bases of the **contract** or **legal obligation** may be used more exceptionally.
→ May be suitable when data is collected directly from people → Often impossible in practice (e.g. when data is collected online)		→ Often adapted for public actors	

Sheet 5 – Carry out a DPIA if necessary (1/2)

Mandatory
For **high-risk processing and high-risk AI systems** according to the AI Regulation

Optional
In other cases

List of criteria

the collection of **sensitive** or **highly personal data;**

large-scale **data processing;**

the collection of data on **vulnerable persons**, such as children;

Cross-referencing of datasets;

Innovative treatments or the use of new technological or organisational measures;

etc.

Sheet 5 – Carry out a DPIA if necessary (1/2)

Mandatory
For **high-risk treatments and high-risk AI systems** according to the AI Regulation

Optional
In other cases

List of criteria

the collection of **sensitive** or **highly personal data;**

large-scale **data processing;**

the collection of data on **vulnerable persons**, such as children;

Cross-referencing of datasets;

Innovative treatments or the use of new technological or organisational solutions;

etc.

Conducting a DPIA is always **a good practice.**

Sheet 5 – Carry out a DPIA if necessary (2/2)

List and assess risks

Plan and implement an action plan

Misuse or misuse of data (data breach);

Automated discrimination;

The production of false content on a real person;

Automated decision-making;

Loss of control over data published online;

Known attacks (data poisoning, backdoor injection, model reversal);

Extraction of training data from the model.

Sheet 5 – Carry out a DPIA if necessary (2/2)

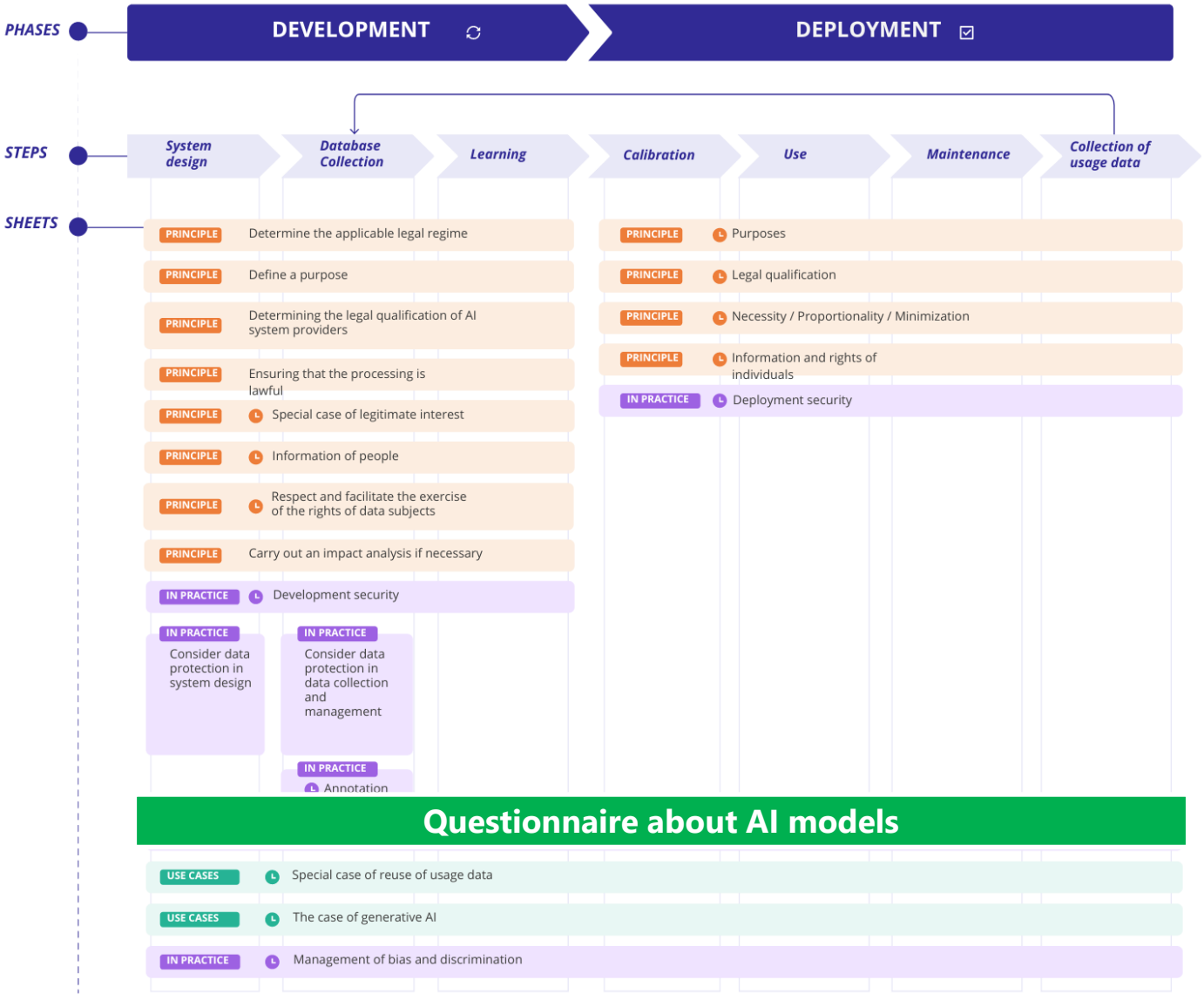
List and assess risks	Plan and implement an action plan
Misuse or misuse of data (data breach);	Provide for measures concerning: **security, minimisation, data protection by design** (anonymisation or pseudonymisation);
Automated discrimination;	Facilitating **the exercise of the rights** of individuals;
The production of false content on a real person;	**the audit and testing** of the system;
Automated decision-making;	**processes and organisation (monitoring** and limiting access to data internally, by third parties and subcontractors);
Loss of control over data published online;	**Governance** (ethical committee);
Known attacks (data poisoning, backdoor injection, model reversal);	**Logging** to identify and explain unusual behaviour;
Extraction of training data from the model.	**Documentation.**

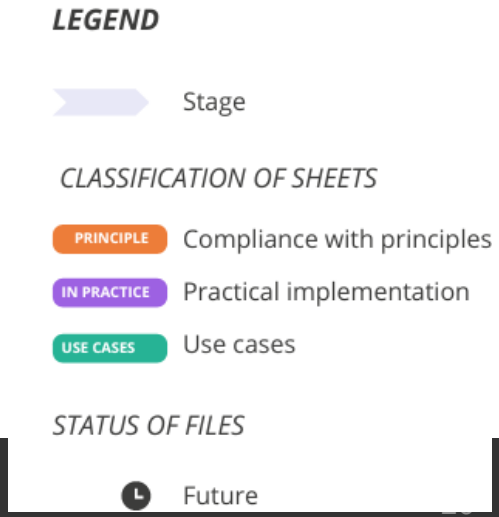
CNIL.

Summary

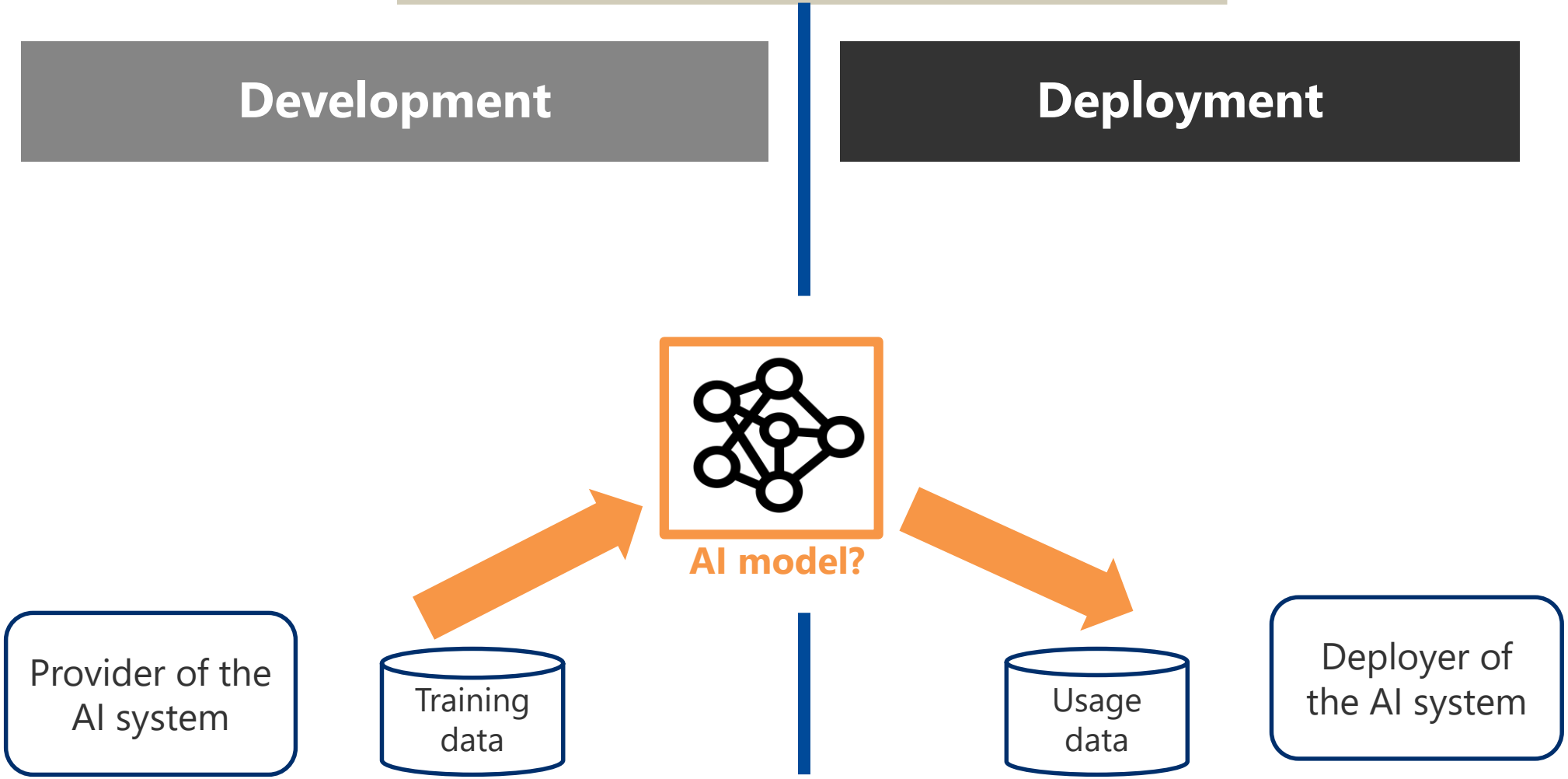
- ✓ Introduction
- ✓ The context of the AI how-to sheets
- ✓ The content of CNIL's recommendations
- ❑ **Recent and future work**

Second batch of how-to-sheets





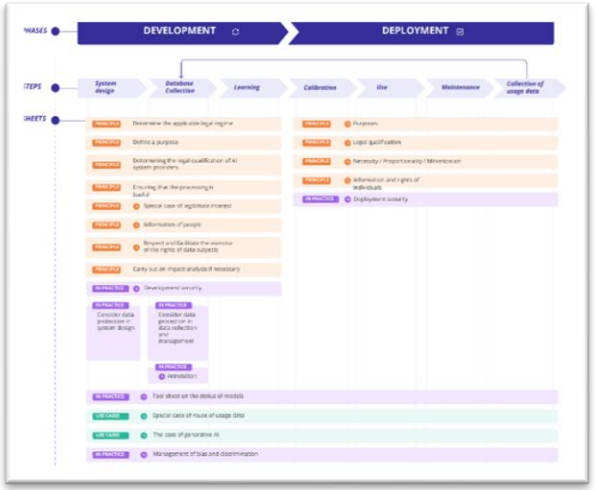
Differences between the two phases



Work and publication to come

- The CNIL **is also continuing its doctrinal work at national level**. This work will be the subject of subsequent publications.

- The CNIL is also actively involved in **the work of the EDPD (guidelines on the interplay between GDPR and European AI Regulation + guidelines on scraping activities in the context of generative AI).**



Any question?

contact:
ia@cnil.fr